Journal für die reine und angewandte Mathematik

A
J 9

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel

H. Hasse L. Schlesinger

Wissenschaftlicher Beirat

H. Brandt / M. Dehn / G. Doetsch / A. Fraenkel / O. Haupt / F. Hausdorff
E. Hellinger / G. Kowalewski / H. Rademacher / K. Reidemeister
A. Rosenthal / C. Schaefer / W. Schmeidler / F. Schottky / O. Toeplitz

Band 166

Heft 1

Ausgegeben den 12. November 1931

A 15

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1931

Band 166. Heft 1.

Inhaltsverzeichnis.

	Seite
Herbrand, J., Sur la non-contradiction de l'Arithmétique	1
Lipka, Stephan, Ein Extremalproblem, nebst Anwendung auf eine Stabilitätsfrage	9
Frucht, Robert, Über die Darstellung endlicher Abelscher Gruppen durch Kollineationen	16
Neiss, F., Darstellung relativ Abelscher Zahlkörper durch Primkörper und Einheitskörper	30
Breuer, Samson, Zyklische Minimalbasis zusammengesetzten Grades	54
v. Török, Elemér, Bemerkungen zu einem Satz von Stickelberger	59
Sidon, S., Verallgemeinerung der in meiner Arbeit „Ein Satz über trigonometrische Polynome mit Lücken und seine Anwendung in der Theorie der Fourier-Reihen" bewiesenen Sätze	62
Estermann, Theodor, Berichtigung zu meiner Arbeit „Über die Darstellungen einer Zahl als Differenz von zwei Produkten"	64

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgend einem Grunde Text-Änderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion ausschließlich unter der Adresse:

An die Redaktion des Journals für die reine und angewandte Mathematik

Professor Dr. Kurt Hensel, Marburg-Lahn, Behringweg 7.

Sur la non-contradiction de l'Arithmétique.

Par *J. Herbrand* † à Paris.

Jacques Herbrand, geboren am 12. Februar 1908 in Paris, verunglückte tödlich bei einer Bergbesteigung in den Alpen am 27. Juli 1931. Am gleichen Tage ging das Manuskript der hier veröffentlichten Arbeit bei der Redaktion ein.

Die letzten 6 Monate seines Lebens verbrachte er an deutschen Universitäten, in enger Berührung und lebhaftem Gedankenaustausch mit einer Reihe deutscher Mathematiker. Tief hat sich ihnen allen seine edle mit reichen wissenschaftlichen Gaben ausgestattete Persönlichkeit eingeprägt. Ein ungewöhnlich begabter Geist ist mit ihm in der Blüte seiner Jugend dahingegangen. Die schönen und wichtigen Resultate, die er auf dem Gebiete der Zahlentheorie und der mathematischen Logik gefunden, und die fruchtbaren Ideen, die er in mathematischen Gesprächen geäußert hat, berechtigten zu den größten Hoffnungen. Die mathematische Wissenschaft hat durch seinen frühzeitigen Tod einen schweren, unersetzlichen Verlust erfahren. Hasse.

Dans deux précédents mémoires[1]) nous avons énoncé et démontré un théorème général permettant de résoudre un grand nombre de questions de Métamathématique, et en avons donné des applications. Nous voulons dans ce travail l'appliquer au problème de la non-contradiction de l'arithmétique plus complètement que nous ne l'avions fait dans D I. Le résultat fondamental est énoncé au début du paragraphe 3.

§ 1. Enoncé d'un théorème général.

Rappelons d'abord l'énoncé du théorème en question.

a) Nous employons les signes de Russell légèrement modifiés: $\vee$, $\sim$, $\times$(et), $\rightarrow$ (pour l'implication), $\equiv$, (Ex) (au lieu de l'E renversé de Russell), (x)[2]); ainsi que les règles de raisonnement de Russell que nous avons d'ailleurs légèrement transformées. En particulier nous n'employons pas dans les propositions la fonction logique ε de Hilbert, et au lieu l'axiome transfini de Hilbert, nous employons les axiomes et règles de Russell qui lui sont équivalents. Nous complétons le formalisme de Russell en admettant l'emploi des fonctions (au sens ordinaire du mot); les fonctions de 0 variable sont les constantes. Pour plus de détails, voir D I, Ch. 1 et 3.

Dans une théorie déterminée, nous avons certaines propositions et certaines fonctions élémentaires, et toutes les propositions que l'on y considère sont des combinaisons

---

[1]) Recherches sur la théorie de la démonstration, Thèse de l'Univ. de Paris, ou Travaux de la Soc. des Sc. et L. de Varsovie (Prace Towazystwa Naukowego) 1930, n 33. Sur le problème fondamental de la Logique Mathématique, Comptes Rendus de la Soc. des Sc. et L. de Varsovie 1931. Ces mémoires seront désignés dans la suite par D I et D II. Nous profiterons de cette occasion pour faire les deux remarques suivantes à leur sujet:

a) Le théorème du Ch. 3, 3.3 de D I n'est exact que si Ax ne contient pas de variables restreintes (ce n'est qu'à cette condition que la réduite de (x) Ax est vraie).

b) Dans D II, au bas de la page 32, nous indiquons que l'on peut "égaler" les éléments d'un champ. Cela demande un éclaircissement, car la valeur des fonctions d'indice n'est pas bien déterminée dans le nouveau champ. Parmi tous les éléments α_i égaux à l'un d'entre eux, nous en choisissons un, β; les β formeront le nouveau champ; dans ce champ, la valeur d'une fonction (descriptive élémentaire, ou d'indice) $f\beta\cdot\beta_2\cdots\beta_n$ sera celui des β qui est égal à la valeur de $f\beta\cdot\beta_2\cdots\beta_n$ dans l'ancien champ; on voit alors que toute proposition vraie dans l'ancien champ, le reste dans le nouveau.

[2]) Nous rappelons que les signes $\times, \rightarrow, \equiv$ peuvent être définis au moyen des signes $\vee$ et $\sim$, seuls considérés comme primitifs. Rappelons leur signification: $\vee$, $\sim$, $\times$, $\rightarrow$, $\equiv$, (Ex), (x), signifient respectivement: ou, non, et, implique, est équivalent à, il existe un x tel que, pour tous les x.

de signes logiques, avec des propositions et des fonctions élémentaires. On a de plus certaines propositions appelées *hypothèses*, et les propositions vraies dans la théorie, sont celles que l'on peut obtenir à partir des hypothèses par application des règles du raisonnement.

Si une proposition peut être démontrée par application de ces règles, sans utiliser d'hypothèse, nous dirons que c'est une identité. Si une proposition P est vraie dans une théorie déterminée, il y a certaines hypothèses $H_1, H_2, \ldots, H_n$ telles que $H_1 \times H_2 \times \cdots \times H_n \cdot \rightarrow P$ soit une identité; et réciproquement (D I, Ch. 3, 2.4), s'il en est ainsi, P est vrai dans la théorie considérée.

La partie d'une proposition sur laquelle s'étend un signe logique, est dite l'*étendue* de ce signe. Ainsi dans $(x) \sim Axy \cdot \vee \cdot (Ey) \sim By$ l'étendue de (x) est $\sim Axy$, celle de (Ey) est $\sim By$, celle du premier $\sim$ est Axy, celle du second $\sim$ est By. Au lieu de l'étendue de (x) ou (Ey), nous dirons aussi l'étendue de x ou y.

Les variables figurant dans les signes de forme (x) et (Ex) seront dites *apparentes*, les autres *réelles*.

Une variable apparente x figurant dans un signe (Ex) situé dans l'étendue d'un nombre pair de signes $\sim$, ou figurant dans un signe (x) situé dans l'étendue d'un nombre impair de signes $\sim$ est dite *restreinte*. Dans les cas contraires, elle est dite *générale*. Ainsi dans $\sim (x)\, Axx \cdot \vee \cdot (Ey) \sim \sim (z)\, Ayz$, x et y sont restreintes, z est générale.

b) Quand une proposition n'a ni variables apparentes ni fonctions, il y a un critère simple pour décider si c'est une identité ou non.

Considérons en effet les propositions élémentaires de cette proposition (elles peuvent contenir des variables ou non; nous considérons évidemment comme identiques celles qui contiennent les mêmes variables dans le même ordre). Attribuons à chacune d'entre elles une *valeur logique*, c'est-à-dire faisons correspondre à chacune un des signes V ou F, et convenons que l'on attribue à toutes les propositions sans variables apparentes formées avec ces propositions, une valeur logique suivant les règles suivantes (voir note 2).

α) Si à P correspond F (ou V), à $\sim P$ correspondra V (ou F).

β) A $P \vee Q$ ne correspond F que si à P et Q correspond F.

On démontre alors (D I, Ch. 1, 5.21) que, pour que P soit une identité, il faut et il suffit que P ait la valeur logique V quelles que soient les valeurs logiques données aux propositions élémentaires. Il faut donc 2^n essais pour décider de la vérité de P, si P contient n propositions élémentaires différentes.

c) Considérons une proposition quelconque P (nous supposons que toutes les variables sont désignées par des lettres différentes). Nous appliquerons les considérations qui vont suivre à la proposition $(x)\,(Ey) \cdot Axy$ prise comme exemple (A est une proposition sans autres variables que x et y, formée avec des propositions et des fonctions élémentaires).

Nous considérerons des fonctions, qui seront d'abord les fonctions élémentaires figurant dans P, puis des fonctions nouvelles obtenues comme suit (il est bien entendu que nous entendons par fonction un pur signe logique, et que nous ne nous occupons pas, du moins pour le moment, de leurs „valeurs"): nous ferons correspondre à toute variable restreinte de P, une fonction dont les arguments sont les variables générales dont l'étendue comprend le symbole (x) ou (Ex) où figure x, et les variables réelles de P; s'il n'y a pas de telles variables restreintes ou réelles, la fonction a 0 argument (une constante). Par exemple pour $(x)\,(Ey) \cdot Axy$, nous aurons la fonction φx correspondant à y.

Considérons maintenant toutes les propositions élémentaires différentes de P (nous considérons cette fois-ci comme identiques deux propositions élémentaires qui ne diffèrent que par leurs variables), soient $A_i x_1 x_2 \cdots x_{n_i}$; et toutes les fonctions différentes

(fonctions élémentaires, ou celles que nous venons d'introduire; même convention), soient $f_i\, x_1\, x_2 \cdots x_{m_i}$. Par exemple si Axy a la forme $Bxx \times Byy \cdot \vee \cdot \sim Bxy$, nous aurons la seule proposition élémentaire Bxy et la seule fonction φx.

Considérons maintenant des ensembles finis de lettres que nous appellerons des champs: $a_0, a_1, \ldots, a_n$; supposons que l'on attribue à chaque $f_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{n_i}}$ une "valeur", c'est-à-dire que l'on fasse correspondre à cet ensemble de signes, un des a_i. Supposons cela réalisé pour certains des $f_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{n_i}}$ (pas forcément pour tous).

Avec toutes nos fonctions élémentaires, nous pouvons en fabriquer d'autres par "substitution"; par exemple avec les fonctions $f_1 x$, $f_2 x$, $f_3 xy$ on peut fabriquer $f_3(f_2 x\, f_1 y)$ et ainsi de suite. Ce qu'il faut entendre par la valeur d'une telle fonction va de soi. Désignons par $F_i\, x_1\, x_2 \cdots x_{p_i}$ une quelconque de ces fonctions (anciennes ou nouvelles).

Nous attribuons à chaque fonction une "*hauteur*" de la manière suivante: les fonctions élémentaires ont une hauteur égale à 1. Si $F_{u_1}, F_{u_2}, \ldots, F_{u_{m_i}}$ ont une hauteur maximum égale à h (les variables sont sous-entendues), alors la hauteur de $f_i\,(F_{u_1}\, F_{u_2} \cdots F_{u_{m_i}})$ est $h + 1$.

Si l'on a dans le champ la valeur d'un nombre de $f_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{m_i}}$ suffisant pour pouvoir calculer la valeur de tous les $F_i\, a_0\, a_0 \cdots a_0$ de hauteur au plus égale à h, et si h est le nombre maximum ayant cette propriété, le champ est dit d'ordre h, et a_0 est l'*élément initial* (cet élément n'est pas toujours univoquement déterminé).

Dans notre exemple, posons $\varphi_1 x = \varphi x$, $\varphi_2 x = \varphi\varphi x, \ldots, \varphi_{n+1} x = \varphi\varphi_n x, \ldots$; alors les fonctions de hauteur au plus égale à h sont $\varphi_1 x, \varphi_2 x, \ldots, \varphi_h x$. Un champ d'ordre h sera constitué par les lettres $a_0, a_1, a_2, \ldots, a_h$ si l'on donne pour valeur à φa_i la valeur a_{i+1} (il nous arrivera souvent d'écrire pour exprimer cela $\varphi a_i = a_{i+1}$). On voit que φa_h n'a pas de valeur dans le champ.

Faisons maintenant correspondre à tout $A_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{n_i}}$ une valeur logique.

Considérons P, et supprimons-y tous les signes de forme (x) et (Ex), puis remplaçons toutes les variables restreintes par la fonction correspondante. Il vient une certaine proposition sans variables apparentes (par exemple $Ax\varphi x$).

Remplaçons les variables par des a_i d'une manière quelconque, et dans l'expression obtenue remplaçons les fonctions de forme $F_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{n_i}}$ par leur valeur (ce n'est pas possible pour tout choix des a_i; dans notre cas on obtiendra $A\, a_i\, a_{i+1}$, et l'opération est impossible quand on remplace x par a_h).

Les $A_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{n_i}}$ ayant une valeur logique, il en est de même de la proposition obtenue. Si cette valeur logique est toujours V, de quelque manière que l'on remplace les variables par des a_i, P est dite vraie dans le champ d'ordre h considéré (on voit que ce champ est caractérisé par les valeurs des fonctions, et les valeurs logiques des $A_i\, a_{\alpha_1}\, a_{\alpha_2} \cdots a_{\alpha_{n_i}}$).

On a alors le théorème fondamental suivant:

α) *Si P est une identité, on peut trouver, connaissant la démonstration de P, un nombre h, tel que $\sim P$ ne puisse être vrai dans un champ d'ordre h.*

β) *Si P n'est pas une identité, on peut construire, quelque soit h, un champ d'ordre h où $\sim P$ est vrai.*

La démonstration et l'énoncé de ce théorème sont intuitionnistes [3]).

---

[3]) Nous entendons par raisonnement intuitionniste, un raisonnement qui satisfait aux conditions suivantes: on n'y considère jamais qu'un nombre fini déterminé d'objets et de fonctions; celles-ci sont bien définies, leur définition permettant de calculer leur valeur d'une manière univoque; on n'affirme jamais l'existence d'un objet sans donner le moyen de le construire; on n'y considère jamais l'ensemble de tous les objets x d'une collection infinie; et quand on dit qu'un raisonnement (ou un théorème) est vrai pour tous ces x, cela signifie que pour chaque x pris en particulier, il est possible de répéter le raisonnement général en question qui ne doit être considéré que comme le prototype de ces raisonnements particuliers.

d) Quand on peut construire pour tout h un champ d'ordre h où P est vrai, nous dirons qu'il y a un *champ infini* où P est *vrai*. Nous dirons que P est *faux* dans un champ infini, si $\sim P$ y est vrai. (Cette expression de champ infini n'est qu'une abréviation; pour avoir le sens intuitionniste des énoncés, il faut revenir aux énoncés précis α et β). On peut alors dire:

Pour que P ne soit pas une identité, il faut et il suffit qu'il y ait un champ infini où P soit faux.

Sous cette forme, le théorème est une précision du théorème connu de Löwenheim-Skolem [4]): quand il y a, en effet, en notre sens, un champ infini où P est vrai, on en déduit aisément, par des procédés non-intuitionnistes, un ensemble dénombrable où P est vrai pour des valeurs déterminées des fonctions, donc une réalisation de P; et réciproquement. Mais:

α) notre énoncé est complètement intuitionniste: on a même le moyen quand on a démontré P, de trouver un nombre h tel que, dans le champ "partiel" d'ordre h, c'est-à-dire au $h^{\text{ième}}$ pas de la construction du champ infini, il soit impossible de rendre P faux.

β) nous ne nous restreignons pas à une forme canonique des propositions, comme Löwenheim, et plus encore, Skolem.

γ) Löwenheim et Skolem supposent implicitement que, quand on a une réalisation de $\sim P$, P ne peut être démontré. Mais c'est là supposer implicitement la non-contradiction des Mathématiques (tout au moins de l'Arithmétique). Notre théorème va nous permettre au contraire d'étudier la non-contracdiction de l'Arithmétique.

e) Considérons maintenant une théorie avec des hypothèses déterminées.

Si l'on peut déterminer un champ infini tel que toutes les hypothèses de la théorie y soient vraies, la théorie n'est pas contradictoire.

Car si la théorie était contradictoire, il y aurait n hypothèses $H_1, H_2, \ldots, H_n$, telles que $\sim \cdot H_1 \times H_2 \times \cdots \times H_n$ soit une identité (voir D I, Ch 5, 6.5). Mais, $H_1, H_2, \ldots, H_n$ étant vrais dans le champ infini, $H_1 \times H_2 \times \cdots \times H_n$ y serait aussi vrai (c'est aisé à voir), donc $\sim \cdot H_1 \times H_2 \times \cdots \times H_n$ y serait faux, ce qui est impossible, si c'est une identité.

Les théorèmes qui précédent ont un grand nombre d'applications (voir D I, et surtout D II). Ils permettent par exemple:

1) de résoudre beaucoup de cas particuliers de l'Entscheidungsproblem.

2) de démontrer rigoureusement (intuitionnistiquement, ce qui n'était pas le cas pour Löwenheim), que l'on peut toujours ramener l'Entscheidungsproblem au cas où il y a seulement *trois propositions élémentaires à deux variables*, ou *une à trois variables*.

Nous allons l'appliquer à la non-contradiction de l'Arithmétique. (Voir déjà D I, Ch. 5, 6.8.)

§ 2. Les axiomes de l'Arithmétique.

La théorie que nous allons étudier et qui est la traduction formelle de l'Arithmétique classique, n'a qu'une seule proposition élémentaire, à deux variables, $x = y$; elle a une constante, 0, une fonction d'une variable, $x + 1$, et d'autres fonctions que nous indiquerons plus loin.

Les hypothèses sont les suivantes:

$$\left.\begin{array}{l} x = x \\ x = y \cdot \rightarrow \cdot y = x \\ x = y \times y = z \cdot \rightarrow \cdot x = z \\ x = y \cdot \equiv \cdot x + 1 = y + 1 \\ \quad \sim \cdot x + 1 = 0 \end{array}\right\} \textbf{Groupe A.}$$

[4]) Voir Löwenheim, Über Möglichkeiten im Relativkalkül, Math. Ann. 76 (1915); et Skolem, Logisch-kombinatorische Untersuchungen ..., Videnskr. Skriften, Math. Naturw. Klasse, Nr. 4, Kristiania 1920.

Puis toutes les hypothèses obtenues en remplaçant, dans la proposition suivante, Φx par une proposition quelconque contenant la variable x:

$$\Phi 0 \times : (x) \cdot \Phi x \to \Phi\ x+1 : \to \cdot (x)\, \Phi x. \quad \textbf{Groupe B} \quad \text{(Induction totale).}$$

On pourra aussi introduire un nombre quelconque de fonctions $f_i\, x_1\, x_2 \cdots x_{n_i}$ avec des hypothèses telles que:

a) *Elles ne contiennent pas de variables apparentes.*

b) *Considérées intuitionnistiquement*[5]*, elles permettent de faire effectivement le calcul de* $f_i x_1\, x_2 \cdots x_{n_i}$*, pour tout système particulier de nombres; et l'on puisse démontrer intuitionnistiquement que l'on obtient un résultat bien déterminé.* **(Groupe C.)**

Comme exemple particulier, supposons que l'on ait déjà introduit un certain nombre de telles fonctions; on pourra alors en introduire une autre fx, avec les nouvelles hypothèses:

$$f0 = \alpha$$
$$f(x+1) = \beta\,(fx),$$

α et βy étant des fonctions formées avec les fonctions déja introduites. C'est le schéma ordinaire de la définition par récurrence.

Mais nous pouvons introduire des schémas de définition bien plus compliqués; par exemple des récurrences multiples portant sur plusieurs variables; nous pouvons ainsi introduire la fonction de Hilbert[6]) avec les hypothèses:

$$\varphi(n+1, a, b) = \varphi(n, a, \varphi(n+1, a, b-1))$$
$$\varphi(n, a, 1) = a$$
$$\varphi(0, a, b) = a + b.$$

Introduisons enfin, d'après Hilbert[7]), un quatrième groupe d'hypothèses, qui n'appartient pas à l'Arithmétique classique.

Ax étant une proposition sans variables apparentes, si, quand on la considère intuitionnistiquement[5]*, on peut démontrer par des procédés intuitionnistes qu'elle est vraie pour tout x, nous ajouterons $(x)\,Ax$ aux hypothèses.* **(Groupe D.)**

§ 3. Le problème de la non-contradiction.

Le résultat fondamental est le suivant:

Les hypothèses A, B, C, D *donnent lieu à une théorie non-contradictoire, si l'on suppose que dans les hypothèses* B, Φx *ne contienne pas de variables apparentes.*

La démonstration est des plus simples.

Pour chaque Φx sans variables apparentes, nous introduisons une nouvelle fonction $\varepsilon\, x y_1\, y_2 \cdots y_n$, les y_i étant les variables de Φx différentes de x. Nous écrirons εx, en sous-entendant ces dernières. Nous introduisons les hypothèses suivantes:

$$\varepsilon 0 = 0 \qquad 1)$$
$$\Phi 0 \cdot \sim \Phi\, x+1 \cdot \varepsilon x = 0 \cdot \to \cdot \varepsilon(x+1) = x+1 \qquad 2)$$
$$\sim [\Phi 0 \cdot \sim \Phi\, x+1 \cdot \varepsilon x = 0] : \to \cdot \varepsilon(x+1) = \varepsilon x \qquad 3)$$
$$\varepsilon x = y+1 \cdot \to : \varepsilon(y+1) = y+1 \times \varepsilon y = 0 \qquad 4)$$

Groupe E.

Traduites en language ordinaire, elles signifient que, si a est le plus petit nombre pour lequel Φa est faux, $\varepsilon x = 0$ pour $x < a$, et $\varepsilon x = a$ pour $x \geqq a$. Si le nombre a n'existe pas, $\varepsilon x = 0$ pour tout x.

On démontre alors que:

---

[5]) Cette expression signifie: traduites en language ordinaire, considérées comme une propriété des entiers, et non comme un pur symbole.

[6]) Hilbert, Über das Unendliche, Math. Ann. **95** (1926).

[7]) Hilbert, Die Grundlagen der elementaren Zahlenlehre, Math. Ann. **104** (1931), p. 491.

a) *Les hypothèses* B *sont une conséquence de ces nouvelles hypothèses.*

Il suffit, pour le voir, de formaliser le raisonnement suivant:

Supposons vrais $\Phi 0$ et $(x) \cdot \Phi x \to \Phi\, x+1$; et supposons qu'il y ait un x tel que $\sim \Phi\, x+1$ soit vrai; il résulte alors de E 2 et 3 que:

$$\varepsilon\,(x+1) = x+1 \quad \text{si} \quad \varepsilon x = 0$$
$$\varepsilon\,(x+1) = \varepsilon x \qquad \text{si} \quad \varepsilon x \neq 0.$$

Posons donc $\varepsilon(x+1) = y+1$. D'après E 4, on aura:

$$\varepsilon(y+1) = y+1$$
$$\varepsilon y \qquad\quad = 0.$$

D'après E 2 et 3, cela entraîne que $\sim \Phi\, y+1$ est vrai (puisque $\Phi 0$ est supposé vrai). On a $y \neq 0$, car sans cela $\Phi 0$ et $\sim \Phi\, 0+1$ seraient vrais, ce qui est contraire à l'hypothèse faite. Donc on peut poser $y = z+1$. D'après cette hypothèse, $\sim \Phi\, z+1$ et $\Phi 0$ seront vrais. E 2 joint au fait que $\varepsilon(z+1) \neq z+1$, entraîne $\varepsilon z \neq 0$; et E 3 entraîne alors que $\varepsilon z = \varepsilon(z+1)$, d'où une contradiction.

b) *Les nouvelles hypothèses sont de la forme* C *si* Φx *ne contient pas de variables apparentes.*

Car dans ce cas on peut reconnaître effectivement si Φx est vrai ou non, et les hypothèses E permettent de calculer effectivement les εx d'une manière univoque et non-contradictoire.

Il suffit donc de démontrer la non-contradiction des hypothèses A, C et D. Mais cela est immédiat sur la base du théorème général. On peut en effet par des procédés intuitionnistes fabriquer un champ d'ordre h composé d'entiers ordinaires, où les hypothèses soient vraies: ce champ est formé des valeurs (au sens intuitif du mot) des fonctions de hauteur au plus égale à h fabriquées avec les fonctions élémentaires, qui se réduisent ici à la fonction $x+1$ et aux fonctions introduites avec les hypothèses C; 0 est élément initial. D'après ce qui a été dit, on peut alors démontrer par des procédés intuitionnistes que toutes les hypothèses sont vraies dans ce champ.

Nous avons dans ce qui précède un procédé pour construire un champ d'ordre h où toutes les hypothèses soient vraies, quelque soit h. Elles sont donc vraies dans un champ infini, et la théorie ne peut être contradictoire (comparer D I, Ch. 5, 6. 8; le raisonnement actuel est plus simple, car nous ramenons les hypothèses B aux hypothèses C).

On voit combien la démonstration est simple, une fois connu le théorème général. Pourtant, la question n'est pas entièrement résolue. Il faut considérer le cas, où dans le groupe B, Φx peut contenir des variables apparentes. Nous pouvons seulement dire:

On peut ajouter sans contradiction les hypothèses B *dans le cas où* Φx *contient des variables apparentes, si la seule fonction intervenant dans* Φx *est (outre la constante* 0), *la fonction* $u+1$.

Nous pouvons en effet introduire la fonction δx avec les hypothèses:

$$\delta 0 = 0$$
$$\delta(x+1) = x.$$

On en déduit la vérité de la proposition:

$$x = 0 \cdot \vee \cdot (Ey)\ x = y+1\,.$$

Nous avons de plus montré dans D I (Ch. 4, 8.1) que les propositions de forme $x \neq x+1+1+\cdots+1$ sont une conséquence d'hypothèses du groupe B, où les Φx n'ont pas de variables apparentes. Enfin nous avons démontré dans D I (Ch. 4, 8.1) que les propositions ci-dessus, jointes aux hypothèses A entraînaient les hypothèses B dans le cas étudié, c. q. f. d.

On aurait un problème encore plus général, en admettant d'autres schémas de définition par récurrence. Par exemple, on pourrait introduire une fonction fx avec les hypothèses:

$$A(f0)$$

$$B[fx, f(x+1)]$$

$(Ex)\ Ax$, et $(x)\ (Ey) \cdot Bxy$ étant des propositions vraies, démontrées sans l'emploi de la nouvelle fonction [8]).

§ 4. Comparaison avec un théorème de M. Gödel.

En raisonnant comme M. Gödel [9]), on peut démontrer que:

Il est impossible de démontrer la non-contradiction d'une théorie par des raisonnements formalisables dans cette théorie, quand cette théorie contient l'Arithmétique.

Le sens exact de cette proposition est aisé à comprendre. Pour des détails, on peut consulter le mémoire de Gödel, où ce théorème est démontré pour le système de Russell et Whitehead. Rappelons en deux mots l'essentiel de son raisonnement:

On peut numéroter intuitionnistiquement toutes les propositions à une variable réelle et toutes les démonstrations de la théorie étudiée. Soit $Pxyz$ une proposition définie de manière intuitionnistique, signifiant: la démonstration numéro x démontre la proposition numéro y, pour la valeur z de sa variable (dans son mémoire, Gödel construit effectivement cette fonction pour la théorie qu'il étudie). Remarquons que le calcul (fait intuitionnistiquement), nécessaire pour vérifier si $Pxyz$ est vrai ou faux, pour des x, y, z, déterminés, peut aussi être fait formellement dans la théorie; donc, si $Pxyz$ est vrai, il est démontrable dans la théorie. Supposons la théorie non-contradictoire. Alors, si β est le numéro de la proposition $(x) \cdot \sim Pxyy$, la proposition $Px\beta\beta$ ne peut être vraie, car cela signifierait que la démonstration numéro x démontre $(x) \cdot \sim Px\beta\beta$, donc on pourrait démontrer $\sim Px\beta\beta$ dans la théorie, et on aurait une contradiction. De plus $(x) \cdot \sim Px\beta\beta$ est indémontrable dans la théorie, car si la démonstration numéro y le démontrait, $Py\beta\beta$ serait vrai (par définition), donc d'après ce que nous avons dit, serait démontrable dans la théorie, et on aurait encore une contradiction. Si l'on formalise dans la théorie les considérations qui précèdent et qui sont intuitionnistes, on a le résultat suivant: w étant la traduction [10]) de la proposition "la théorie n'est pas contradictoire", $w \rightarrow \sim Px\beta\beta$ est une proposition vraie de la théorie (x étant une variable). Si w était démontrable dans la théorie, il en serait donc de même de $\sim Px\beta\beta$, donc de $(x) \cdot \sim Px\beta\beta$, et nous venons de voir que cela entraînait une contradiction dans la théorie. Donc *w est indémontrable.*

Appliquons cette méthode à l'Arithmétique avec les hypothèses A, B, et C (laissons de côté les hypothèses D pour simplifier). Nos raisonnements, et ceux nécessaires pour établir le théorème fondamental, sont formalisables dans cette théorie. Mais, si nous voulons appliquer le raisonnement de Gödel, il est nécessaire de considérer une théorie

---

[8]) M. Bernays nous signale que si l'on avait démontré la non-contradiction d'une Arithmétique comportant les hypothèses A, B et comme fonctions, celles intervenant dans Ax et Bxy, l'addition et la multiplication il en résulterait que l'on peut ajouter les nouvelles hypothèses sans contradiction, car tout raisonnement fait avec la nouvelle fonction fx, peut se faire dans l'Arithmétique que nous venons de décrire.

[9]) Gödel, Über formal unentscheidbare Sätze ..., Monatshefte für Math. und Ph. **38** (1931), p. 173. Pour comprendre cette proposition, il faut se figurer tous les signes qui interviennent dans la Métamathématique représentés par des objets de la théorie en question, par exemple par des nombres entiers en Arithmétique; les propriétés de ces signes, et leurs relations entre eux, seront alors représentées par certaines propositions de la théorie; et tout raisonnement de la théorie en question fait avec ces objets et ces propositions, correspondra à un raisonnement métamathématique, dont il sera en quelque sorte la traduction.

[10]) Voir la note 9.

déterminée. Dans le groupe C, nous n'avons qu'une description d'hypothèses que l'on peut introduire. Il faut considérer un groupe déterminé de schémas d'hypothèses du type C, soit le groupe C′. Si l'on veut faire le raisonnement de Gödel, nous allons voir qu'il faut introduire d'autres schémas de définition de fonctions; il est donc impossible d'appliquer ses considérations à notre Arithmétique.

On pourrait objecter: il est peut-être possible de décrire d'un seul coup tous les schémas de fabrication de fonctions inclus dans C. Cela voudrait dire: il est possible de décrire d'un seul coup tous les procédés intuitionnistes de fabriquer des fonctions d'entiers. Mais cela est impossible. Car dans ce cas, on pourrait, par un procédé intuitionniste, numéroter toutes celles de ces fonctions n'ayant qu'une variable, soient $f_1x, f_2x, \ldots, f_nx, \ldots$ $f_xx + 1$ serait alors une fonction définie intuitionnistiquement, qui ne ferait pas partie des précédentes, d'où une contradiction.

Appliquons cette considération à toutes les fonctions définissables par C′ et celles obtenues en les combinant entre elles et avec $x + 1$. La fonction $f_xx + 1$ ne peut donc faire partie de ces dernières. Or pour faire le raisonnement de Gödel, il faut numéroter tous les objets intervenant dans les démonstrations; on est donc conduit à fabriquer la fonction de deux variables f_yx: cela justifie ce que nous disions plus haut: il est impossible de formaliser dans une Arithmétique avec les hypothèses C′, le raisonnement de Gödel relatif à cette Arithmétique.

Faisons encore deux remarques:

a) Tout raisonnement intuitionniste peut toujours être fait avec des entiers ordinaires, car on peut toujours remplacer les objets que l'on y considère par des entiers ordinaires, en les numérotant, par exemple. Il nous semble à peu près certain que tout raisonnement intuitionniste peut alors être fait dans une Arithmétique avec les hypothèses A, B et C. Mais la justification de ce point (une *démonstration*, au sens mathématique du mot, est évidemment impossible, comme pour toute affirmation portant sur l'ensemble de *tous* les raisonnements intuitionnistes), nous entraînerait à une discussion détaillée sur laquelle nous reviendrons peut-être une autre fois. Il en résulterait que les hypothèses du groupe D résultent des précédentes.

b) Il nous parait impossible, contrairement à l'opinion de Gödel [11]), qu' il y ait des raisonnements intuitionnistes non formalisables en analyse ordinaire. C'est ainsi que nous croyons que l'Arithmétique avec les hypothèses A, B, C, D, est une partie de l'analyse ordinaire. Il nous parait probable que la position de cette question est la suivante: on ne pourra jamais donner d'exemple de raisonnement intuitionniste non formalisable en analyse ordinaire, et il sera également toujours impossible de démontrer qu'il n'en existe pas: nous avons en effet montré qu'il était impossible de décrire tous les procédés de raisonnement intuitionnistes (puisqu'il est impossible de décrire tous les procédés de fabrication de fonctions). *Il peut y avoir là une sorte de postulat logique.* Il en résulterait qu'il est impossible de démontrer la non-contradiction de l'analyse ordinaire.

Il n'est même pas impossible que tout raisonnement intuitionniste puisse se faire dans une Arithmétique avec les hypothèses A, B et en n'admettant dans C que l'addition et la multiplication ordinaires [12]). S'il en était ainsi, la non-contradiction de l'Arithmétique ordinaire serait déjà indémontrable.

---

[11]) Loco citato note 9, p. 197.

[12]) Comparer Gödel, loco citato, Satz 7; et la note 8 du présent travail.

Göttingen, den 14. Juli 1931.

Eingegangen 27. Juli 1931.

Ein Extremalproblem, nebst Anwendung auf eine Stabilitätsfrage.

Von *Stephan Lipka* in Szeged (Ungarn).

1. Die Gleichgewichtslage eines mechanischen Systems hat an irgendeiner Stelle den Charakter der Stabilität, wenn das System die folgenden Eigenschaften besitzt: Es bleibt während seiner Bewegung in der Nähe der erwähnten Stelle, wenn wir die Punkte des Systems von der ursprünglichen Lage hinreichend wenig verrücken und den Punkten genügend kleine Anfangsgeschwindigkeiten geben.

Unsere Betrachtungen beginnen mit einer Stabilitätsfrage, welche zu einem Extremalproblem führt. Wir betrachten natürlich-konservative mechanische Systeme. Ein mechanisches System ist natürlich-konservativ, wenn das Energieintegral die Form $T + V =$ constans hat, wo T, die kinetische Energie, ein Ausdruck zweiten Grades der Geschwindigkeiten ist, und V, die potentielle Energie, bloß diejenigen Koordinaten enthält, welche die Lage des Systems bestimmen. Auf solche Systeme bezieht sich der folgende Satz von Lagrange, welchen zum erstenmal Dirichlet streng bewiesen hat[1]). *Wenn die Potentialfunktion an irgend einer Stelle ein isoliertes Maximum hat, dann ist das System ebendort in stabiler Gleichgewichtslage.* Statt Maximum der Potentialfunktion können wir von Minimum der potentiellen Energie sprechen. Im Falle der natürlich-konservativen Systeme enthalten die Beziehungen zwischen den Koordinaten die Zeit nicht. Diese Beziehungen sind gewöhnlich durch Gleichungen gegeben, mit deren Hilfe die Anzahl der Koordinaten reduziert werden kann derart, daß die übrigbleibenden Koordinaten voneinander unabhängig werden. Dann wird also auch die Potentialfunktion nur voneinander unabhängige Veränderliche enthalten, so daß die Stabilitätsfrage mittels des Lagrange-Dirichletschen Satzes auf eine gewöhnliche Extremalaufgabe zurückgeführt wird. Wir werden in den folgenden Überlegungen voraussetzen, daß die Beziehungen zwischen den Koordinaten, welche die Lage des Systems bestimmen, von ganz allgemeiner Natur sind, also daß diese Beziehungen nicht nur Gleichungen, sondern auch Ungleichungen enthalten können. Beziehungen von dieser Art drücken bekanntlich ganz allgemeine Zwangsbedingungen aus. Die Betrachtungsweise von Dirichlet läßt sich auch auf solche Systeme übertragen und ergibt, daß die Gleichgewichtslage an irgendeiner Stelle stabil ist, wenn die Potentialfunktion ebendort ein relatives Maximum hat unter der Bedingung, daß die entsprechenden Gleichungen und Ungleichungen erfüllt sind. Also können wir unser Problem folgendermaßen formulieren. Es sei die Funktion $V(q_1, q_2, \ldots, q_n)$ nach den Veränderlichen $q_1, q_2, \ldots, q_n$ zweimal stetig differenzierbar. Die Veränderlichen sollen in der Umgebung der Stelle $(q_1^0, q_2^0, \ldots, q_n^0) = (q_i^0)$ dem Ungleichungssystem

$$\text{(I)} \qquad \begin{aligned} f_1(q_1, \ldots, q_n) &\geqq 0 \\ &\vdots \\ f_k(q_1, \ldots, q_n) &\geqq 0 \end{aligned}$$

$$0 < k < n$$

[1]) L. Dirichlet, Über die Stabilität des Gleichgewichtes, dieses Journal **32** (1846), S. 85.

genügen. An der Stelle (q_i^0) sei $f_1(q_1^0, \ldots, q_n^0) = \cdots = f_k(q_1^0, \ldots, q_n^0) = 0$. [2]) Wir setzen voraus, daß die Relationen (I) keine Gleichung enthalten, weil eine Gleichung nur eine Verminderung der Anzahl der unabhängigen Veränderlichen bedeutet. Die Funktionen $f_1, f_2, \ldots, f_k$ seien zweimal stetig differenzierbar, und die Funktionalmatrix

$$\left\| \frac{\partial f_h}{\partial q_j} \right\| \qquad h = 1, 2, \ldots, k; \quad j = 1, 2, \ldots, k, \ldots, n$$

habe an der Stelle (q_i^0) den Rang k; wir können sogleich ohne Beschränkung der Allgemeinheit annehmen, daß die Jacobische Determinante $\frac{\partial(f_1, \ldots, f_k)}{\partial(q_1, \ldots, q_k)}$ an der Stelle (q_i^0) von Null verschieden sei. Unser Problem ist nun folgendes: *Unter welchen Bedingungen hat die Funktion* $V(q_1, q_2, \ldots, q_n)$ *an der Stelle* (q_i^0) *einen bedingten Extremalwert, und zwar einen solchen, welcher den Relationen* (I) *entspricht*? Wir führen neue Koordinaten ein und betrachten zu diesem Zwecke das Funktionensystem

$$\begin{aligned} x_1 &= f_1(q_1, \ldots, q_n) \\ &\vdots \qquad\qquad x_i^0 = f_i(q_1^0, \ldots, q_n^0) \\ &\vdots \qquad\qquad (i = 1, 2, \ldots, k) \\ x_k &= f_k(q_1, \ldots, q_n) \\ x_{k+1} &= q_{k+1} \\ &\vdots \qquad\qquad x_i^0 = q_i^0 \\ &\vdots \qquad\qquad (i = k+1, k+2, \ldots, n) \\ x_n &= q_n \,. \end{aligned}$$

Die Jacobische Determinante dieses Funktionensystems ist an der Stelle (q_i^0) nach den Voraussetzungen von Null verschieden, also läßt sich das Funktionensystem in der Nähe der Stelle $(x_1^0, \ldots, x_n^0)$ nach $q_1, \ldots, q_n$ auflösen und wird

$$(1) \qquad q_i = \varphi_i(x_1, x_2, \ldots, x_n) \qquad (i = 1, 2, \ldots, n)$$

wo die $\varphi_i(x_1, \ldots, x_n)$ eindeutige und nach den Variabeln x_i zweimal stetig differenzierbare Funktionen sind. Jetzt werden die Veränderlichen x_i mittels der Gleichungen (1) in die Funktion $V(q_1, \ldots, q_n)$ eingeführt; wir gewinnen damit eine neue Funktion $g(x_1, x_2, \ldots, x_n)$. Der Variabilitätsbereich der Veränderlichen x_i ist nach (I)

$$(2) \qquad x_1 \geqq 0, \quad x_2 \geqq 0, \ldots, x_k \geqq 0,$$

die Veränderlichen $x_{k+1}, x_{k+2}, \ldots, x_n$ können beliebige Werte annehmen. Wenn also die Funktion $g(x_1, \ldots, x_n)$ an der Stelle (x_i^0) einen Extremalwert besitzt, welcher den Bedingungen (2) entspricht, dann hat die Funktion $V(q_1, \ldots, q_n)$ einen der Bedingungen (I) entsprechenden Extremalwert an der Stelle (q_i^0). *Wir haben also zu untersuchen, wann die Funktion* $g(x_1, \ldots, x_n)$ *ein relatives Extremum* (*z. B. Minimum*) *hat, welches den Bedingungen* (2) *entspricht.* Im Falle eines Minimums folgt aus der Entwicklung

$$g(x_1^0 + \delta x_1, \ldots, x_n + \delta x_n) - g(x_1^0, \ldots, x_n^0) = \sum_{(i)} \frac{\partial g}{\partial x_i}_{(x_i = x_i^0)} \delta x_i + \frac{1}{2} \sum_{(i,j)} \left(\frac{\partial^2 g}{\partial x_i \, dx_j} \right)' \delta x_i \, \delta x_j \, [3]) \,,$$

daß die ersten partiellen Derivierten an der Stelle (x_i^0) den Bedingungen

$$(3) \qquad \begin{aligned} \frac{\partial g}{\partial x_j} &\geqq 0 \qquad & j &= 1, 2, \ldots, k \\ \frac{\partial g}{\partial x_h} &= 0 \qquad & h &= k+1, \ldots, n \end{aligned}$$

---

[2]) Wäre nämlich eine der Funktionen von (I) an der Stelle (q_i^0) positiv, dann würde diese Funktion in einer ganzen Umgebung dieser Stelle nur positive Werte annehmen, so daß die entsprechende Ungleichung für die Veränderlichen keine Einschränkung bedeuten würde.

[3]) Der Strich bedeutet, daß die Derivierten irgendwo zwischen den Stellen (x_i^0) und $(x_i^0 + \delta x_i)$ zu nehmen sind.

genügen. Wenn eine der Derivivierten (3) bestimmt positiv ist, dann hat die Funktion $g(x_1, \ldots, x_n)$ an der Stelle (x_i^0) ein Minimum, im entgegengesetzten Falle, also wenn die Derivierten (3) alle verschwinden, muß für die Werte

$$\delta x_1 \geqq 0, \ldots, \delta x_k \geqq 0, \quad \delta x_{k+1}, \ldots, \delta x_n$$

der Veränderlichen die quadratische Form

$$\sum_{(ij)} \frac{\partial^2 g}{\partial x_i dx_j} \delta x_i \, \delta x_j$$

positiv sein, damit die Funktion $g(x_1, \ldots, x_n)$ an der Stelle (x_i^0) ein relatives Minimum besitzt. Um unsere Aufgabe zu vereinfachen, bedeute ε_i eine Veränderliche, welche die Werte $+1$ und -1 annimmt, so daß die Folge $\varepsilon_{k+1}, \varepsilon_{k+2}, \ldots, \varepsilon_n$ die aus den beiden Elementen $+1$, -1 gebildeten Variationen $(n-k)$-ter Ordnung mit Wiederholung repräsentiere. Die Anzahl dieser Variationen ist 2^{n-k}. Es sei noch $\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_k = 1$. Wir betrachten die Gesamtheit der quadratischen Formen

$$\sum_{(i)} \varepsilon_i y_i (a_{i1} y_1 \varepsilon_1 + a_{i2} y_2 \varepsilon_2 + \cdots + a_{in} y_n \varepsilon_n) = \sum_{(i,j)} \varepsilon_i \varepsilon_j a_{ij} y_i y_j \quad (i, j = 1, 2, \ldots, n).$$

Die Anzahl dieser Formen ist auch 2^{n-k}. Wenn nun die Veränderlichen y_i den Bedingungen

$$y_1 \geqq 0, \quad y_2 \geqq 0, \ldots, y_n \geqq 0$$

genügen, so ist der Wertevorrat der Gesamtheit dieser Formen ersichtlich identisch mit dem Wertevorrat der quadratischen Form

$$\sum_{(i,j)} a_{ij} x_i x_j ,$$

wo bei die n Veränderlichen nur die Bedingungen

$$x_1 \geqq 0, \quad x_2 \geqq 0, \ldots, x_k \geqq 0 \qquad k < n$$

erfüllen. *Es soll also die notwendige und hinreichende Bedingung dafür entwickelt werden, daß eine quadratische Form* $\sum_{(i,j)} a_{ij} x_i x_j$ *für*

$$x_1 \geqq 0, \quad x_2 \geqq 0, \ldots, x_n \geqq 0$$

positiv sei. Der Fall $x_1 = x_2 = , \ldots, = x_n = 0$ bildet selbstverständlich eine Ausnahme. Eine Form, welche diese Eigenschaft besitzt, nennen wir eine *relativ definite positive Form*

2. In betreff dieses Problems muß ich zunächst erwähnen, daß G. Pólya [4]) neuerdings den folgenden wichtigen Satz bewiesen hat: Eine Form in n Variabeln $x_1, x_2, \ldots, x_n$ die für alle nichtnegativen Wertsysteme der Variabeln, mit Ausnahme des identisch verschwindenden Wertsystems, positive Werte annimmt, läßt sich als Quotient zweier Formen mit lauter positiven Koeffizienten darstellen. Pólya hat unter anderem bewiesen, daß wenn eine Form die erwähnte Eigenschaft besitzt, dann aus der Form bei wiederholter Multiplikation mit $x_1 + x_2 + \cdots + x_n$ schließlich eine Form mit lauter positiven Koeffizienten hervorgehen muß. Wenn also eine quadratische Form relativ definit positiv ist, kann man diese Eigenschaft in einer endlichen Anzahl von Schritten bestätigen. Wir wollen aber hier eine solche Methode entwickeln, welche *bloß mit Hilfe der Koeffizienten* der quadratischen Form, und zwar *mit einer endlichen Anzahl von Schritten* darüber entscheidet, ob die Form relativ definit positiv ist, oder nicht.

Wir betrachten zuerst unsere Aufgabe in einem speziellen Falle, und werden in diesem Paragraphen voraussetzen, daß *die Hauptminoren* der Diskriminante der quadratischen Form, *alle von Null verschieden sind.* Es sei noch bemerkt, daß unsere Methode auch zur Beantwortung jener Frage geeignet ist, wann eine quadratische Form (im gewöhnlichen Sinne) positiv definit ist.

[4]) G. Pólya, Über positive Darstellung von Polynomen, Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich **73** (1928).

Das aufgeworfene Problem wird auf eine Minimumaufgabe zurückgeführt, und zwar: Das Wertsystem $x_1, x_2, \ldots, x_n$ bezeichne einen Punkt des n-dimensionalen Raumes. Wir betrachten den Wert der quadratischen Form in jenen Punkten, welche in dem ersten 2^n-ten Teil (also in dem Teil $x_1 \geqq 0, x_2 \geqq 0, \ldots, x_n \geqq 0$) des n-dimensionalen Raumes liegen. Wenn wir die folgenden Transformationen

$$x_i = \varrho y_i \qquad i = 1, 2, \ldots, n$$
$$\varrho = \text{Max } (x_1, x_2, \ldots, x_n)$$

einführen, so geht, da $0 \leqq y_i \leqq 1$ ist, der jetzt erwähnte unendliche Raumteil in eine beschränkte Menge über. Diese Menge ist die Vereinigungsmenge der folgenden $n-1$ dimensionalen Mengen:

$$\begin{array}{ll}
(e_1) & y_1 = 1, \quad 0 \leqq y_2 \leqq 1, \ldots, 0 \leqq y_n \leqq 1 \\
(e_2) & 0 \leqq y_1 \leqq 1, \quad y_2 = 1, \ldots, 0 \leqq y_n \leqq 1 \\
\vdots & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
(e_n) & 0 \leqq y_1 \leqq 1, \quad 0 \leqq y_2 \leqq 1, \ldots, \quad y_n = 1 .
\end{array}$$

Diese Mengen sind Seiten des n-dimensionalen Einheitswürfels. Die Vereinigungsmenge dieser Seiten sei mit (e) bezeichnet. Die Formel

$$\sum_{(i\,j)} a_{ij}\, x_i\, x_j = Q(x, x_2, \ldots, x_n) = \varrho^2 Q(y_1, y_2, \ldots, y_n)$$

zeigt, daß wir uns in der Folge auf die Menge (e) beschränken können. Wir werden infolgedessen die notwendige und hinreichende Bedingung dafür entwickeln, daß die quadratische Form in jeder der vorigen $(n-1)$-dimensionalen Seiten eine positive untere Grenze habe. Wir betrachten also irgendwelche Teile (e_i), und bezeichnen mit G den Punkt von (e_i), in welchem der quadratische Ausdruck

$$Q(y_1, y_2, \ldots, y_{i-1}, \ 1, \ y_{i+1}, \ldots, y_n) = Q_{y_i}$$

seine untere Grenze annimmt. Der Punkt G kann ein innerer Punkt von (e_i) sein, oder kann in einer $(n-k)$-dimensionalen Seite von (e_i) liegen. Unter einer $(n-k)$-dimensionalen Seite von (e_i) verstehen wir die folgende:

$$(e_i') \qquad \begin{array}{l} y_{r_1} = y_{r_2} = \cdots = y_{r_\nu} = y_i = 1 \\ y_{\varrho_1} = y_{\varrho_2} = \cdots = y_{\varrho_\mu} = 0 \end{array} \qquad \nu + \mu = k - 1$$

$$0 \leqq y_j \leqq 1, \quad \text{wenn} \quad j \neq r_1, r_2, \ldots, r_\nu, i, \varrho_1, \varrho_2, \ldots, \varrho_\mu .$$

Wenn der Punkt G ein innerer Punkt von (e_i) ist, dann hat Q_{y_i} im Punkte G ein lokales Minimum. Der Ausdruck Q_{y_i} kann also seine untere Grenze nur in einem solchen Punkte annehmen, in welchem Q_{y_i} entweder ein lokales Minimum besitzt, oder welcher in einer Seite von (e_i) liegt. Der Ausdruck Q_{y_i} hat dann und nur dann ein lokales Minimum in (e_i), oder an ihrer Grenze, wenn die folgenden beiden Bedingungen erfüllt sind:

1. Das Gleichungssystem

$$\begin{array}{l}
\frac{1}{2}\frac{\partial Q_{y_i}}{\partial y_1} = a_{11}y_1 + a_{12}y_2 + \cdots + a_{1,i-1}y_{i-1} + a_{1,i+1}y_{i+1} + \cdots + a_{1n}y_n + a_{1i} = 0 \\
\qquad\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
\frac{1}{2}\frac{\partial Q_{y_i}}{\partial y_{i-1}} = a_{i-1\,1}y_1 + a_{i-1,2}y_2 + \cdots + a_{i-1,i-1}y_{i-1} + a_{i-1,i+1}y_{i+1} + \cdots + a_{i-1\,n}y_n + a_{i-1,i} = 0 \\
\frac{1}{2}\frac{\partial Q_{y_i}}{\partial y_{i+1}} = a_{i+1,1}y_1 + a_{i+1,2}y_2 + \cdots + a_{i-1,i+1}y_{i-1} + a_{i+1,i-1}y_{i+1} + \cdots + a_{i+1,n}y_n + a_{i+1,i} = 0 \\
\qquad\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
\frac{1}{2}\frac{\partial Q_{y_i}}{\partial y_n} = a_{n,1}y_1 + a_{n2}y_2 + \cdots + a_{n,i-1}y_{i+1} + a_{n,i+1}y_{i+1} + \cdots + a_{nn}y_n + a_{ni} = 0
\end{array}$$

besitzt eine solche Lösung $y_1^*, \ldots, y_{i-1}^*, y_{i+1}^*, \ldots, y_n^*$, für welche die Relation

$$1 \geqq y_j^* \geqq 0$$

gilt[5]).

2. Die Determinante des vorigen Gleichungssystems stellt die Diskriminante einer positiv definiten quadratischen Form in $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n$ dar.

Wenn 1. und 2. erfüllt sind, dann nimmt Q_{y_i} wirklich seine untere Grenze in dem Punkte $y_1^*, \ldots, y_{i-1}^*, y_{i+1}^*, \ldots, y_n^*$ an, weil nach 2. die Ungleichung

$$Q(y_1^* + y_1, \ldots, y_{i-1}^* + y_{i-1}, 1, y_{i+1}^* + y_{i+1}, \ldots, y_n^* + y_n) = Q(y_1^*, \ldots, y_{i-1}^*, 1, y_{i+1}^*, \ldots, y_n^*) + \sum_{(h,j \neq i)} a_{hj} y_h y_j > Q(y_1^*, \ldots, y_{i-1}^*, 1, y_{i+1}^*, \ldots, y_n^*)$$

gilt. Wenn von den Bedingungen 1. und 2. eine nicht erfüllt ist, dann wird Q_{y_i} seine untere Grenze gewiß in einer $(n-k)$-dimensionalen Seite (e_i') von (e_i) annehmen. Es ist möglich, daß diese Seite aus einem einzigen Punkte besteht; in diesem Falle wird Q_{y_i} seine untere Grenze in einem Eckpunkte des n-dimensionalen Einheitswürfels annehmen. Wenn die betreffende Seite $(n-k>0)$-dimensional ist, dann wird die untere Grenze in einem inneren Punkte dieser Seite (e_i') angenommen. In diesem Punkte von (e_i) muß der quadratische Ausdruck

$$Q(y_1, \ldots, y_{i-1}, 1, y_{i+1}, \ldots, y_n) = \bar{Q}(y_{\lambda_1}, y_{\lambda_2}, \ldots, y_{\lambda_{n-k}})$$

$$y_{r_1} = y_{r_2} = \cdots = y_{r_\nu} = 1 \qquad \nu + \mu = k - 1$$
$$y_{\varrho_1} = y_{\varrho_2} = \cdots = y_{\varrho_\mu} = 0$$

ein lokales Minimum haben, demnach soll

A) das Gleichungssystem

$$\frac{1}{2}\frac{\partial \bar{Q}}{\partial y_{\lambda_1}} = 0, \quad \frac{1}{2}\frac{\partial \bar{Q}}{\partial y_{\lambda_2}} = 0, \ldots, \frac{1}{2}\frac{\partial \bar{Q}}{\partial y_{\lambda_{n-k}}} = 0$$

eine Lösung besitzen, für welche die Relation

$$1 > y_{\lambda_1}^* > 0, \quad 1 > y_{\lambda_2}^* > 0, \ldots, 1 > y_{\lambda_{n-k}}^* > 0$$

gilt.

B) Es soll die Determinante des vorigen Gleichungssystems die Diskriminante einer positiv definiten quadratischen Form von $n-k$ Veränderlichen sein.

Also läßt sich unsere Aufgabe nach den vorangeführten Überlegungen auf die folgende Weise lösen: *Betrachten wir alle möglichen Gleichungssysteme*

$$\begin{aligned}
a_{\lambda_1\lambda_1} y_{\lambda_1} + a_{\lambda_1\lambda_2} y_{\lambda_2} + \cdots + a_{\lambda_1\lambda_\varkappa} y_{\lambda_\varkappa} &= -\sum_{k=1}^{\nu} a_{\lambda_1 r_k} \\
a_{\lambda_2\lambda_1} y_{\lambda_1} + a_{\lambda_2\lambda_2} y_{\lambda_2} + \cdots + a_{\lambda_2\lambda_\varkappa} y_{\lambda_\varkappa} &= -\sum_{k=1}^{\nu} a_{\lambda_2 r_k} \qquad (4) \\
&\vdots \\
a_{\lambda_\varkappa\lambda_1} y_{\lambda_1} + a_{\lambda_\varkappa\lambda_2} y_{\lambda_2} + \cdots + a_{\lambda_\varkappa\lambda_\varkappa} y_{\lambda_\varkappa} &= -\sum_{k=1}^{\nu} a_{\lambda_\varkappa r_k},
\end{aligned}$$

wo $1 \leqq \varkappa < n$, $1 \leqq \nu \leqq n - \varkappa$, *ferner* $r_k \neq \lambda_1, \lambda_2, \ldots, \lambda_\varkappa$ $(k = 1,2, \ldots, \nu)$ *ist.*

Die Anzahl solcher Systeme ist $\sum_{i=1}^{n-1} \binom{n}{i} \sum_{k=0}^{n-i-1} \binom{n-i}{k} = 3^n - 2^{n+1} + 1$. *Es bezeichne* $(y_{\lambda_i}^*)$ *die Lösung des Gleichungssystems* (4), *ferner* $Q(y_{\lambda_1}, y_{\lambda_2}, \ldots, y_{\lambda_\varkappa})$ *den quadratischen Ausdruck, welchen man aus* $Q(y_1, y_2, \ldots, y_n)$ *durch die Substitution*

---

[5]) Die Determinante des Gleichungssystems ist ein Hauptminor der Diskriminante, also von Null verschieden.

$$y_{\varrho_1} = y_{\varrho_2} = \cdots = y_{\varrho_\mu} = 0 \qquad \mu = n - \varkappa - \nu$$
$$y_{r_1} = y_{r_2} = \cdots = y_{r_\nu} = 1 \qquad \varrho_i \neq \lambda_1, \lambda_2, \ldots, \lambda_\varkappa, r_1, r_2, \ldots, r_\nu; \quad i = 1,2,\ldots,\mu$$

gewinnt. Wir behaupten, daß die quadratische Form dann und nur dann für positive Werte der Veränderlichen positiv ist, wenn

I. *Jede solche Lösung von* (4) *für welche* $y^*_{\lambda_i} \geqq 0$ *ist, der Ungleichung*

$$Q(y^*_{\lambda_1}, y^*_{\lambda_2}, \ldots, y^*_{\lambda_\varkappa}) > 0$$

genügt.

II. *Die quadratische Form besitzt in jedem Eckpunkte des n-dimensionalen Einheitswürfels, außer dem Punkte* $(0, 0, \ldots, 0)$, *einen positiven Wert.*

Die Notwendigkeit der Bedingungen I., II. ist klar. Aus den obigen Überlegungen folgt auch, daß die Bedingungen I., II. hinreichend sind. Nimmt nämlich $Q(y_1, y_2, \ldots, y_n)$ seine untere Grenze in einem inneren Punkte irgendeiner Seite (e_i) oder (e'_i) an (siehe A) und B)), so ist diese untere Grenze nach I. positiv. Sie ist nach II. gleichfalls positiv, wenn sie in einem Eckpunkte des Würfels angenommen wird.

3. Wir haben in den vorigen Überlegungen vorausgesetzt, daß *alle Hauptminoren* der Diskriminante der quadratischen Form *von Null verschieden sind.* Zufolge dieser Voraussetzung war die Anzahl der lokalen Minimumstellen der quadratischen Form höchstens eins; was auch bei der Bedingung I. ausgenützt wurde. Wir werden jetzt voraussetzen, daß unter den genannten Hauptminoren gewisse gleich Null sind, also daß unter den Gleichungssystemen (4) einzelne eine verschwindende Determinante haben. Unter diesen Gleichungssystemen betrachten wir auch nur diejenigen, die auflösbar sind. Wir betrachten im folgenden ein solches Gleichungssystem.

4. Die Matrix der Koeffizienten habe den Rang $r < \varkappa$. Man gewinnt nach einer gewissen Vertauschung der Indizes $\lambda_1, \lambda_2, \ldots, \lambda_\varkappa$ für alle Lösungen von (4) die Ausdrücke

$$(5) \qquad y_{\lambda_k} = b_k + c_{k_1} y_{\lambda_{r+1}} + c_{k_2} y_{\lambda_{r+2}} + \cdots + c_{k,\varkappa-r} y_{\lambda_\varkappa} \qquad k = 1, 2, \ldots, r,$$

wo man die Werte für $y_{\lambda_{r+1}}, y_{\lambda_{r+2}}, \ldots, y_{\lambda_\varkappa}$ beliebig wählen darf. Wenn wir die linearen Ausdrücke (5) in den quadratischen Ausdruck

$$Q(y_1, y_2, \ldots, y_n) = \bar{Q} \qquad r_j \neq \lambda_1, \lambda_2, \ldots, \lambda_\varkappa \quad j = 1, 2, \ldots, \nu$$
$$y_{r_1} = y_{r_2} = \cdots = y_{r_\nu} = 1 \qquad \varrho_i \neq r_1, r_2, \ldots, r_\varkappa$$
$$y_{\varrho_1} = y_{\varrho_2} = \cdots = y_{\varrho_\mu} = 0 \qquad \mu + \nu = n - \varkappa \qquad \varrho_i \neq \lambda_1, \lambda_2, \ldots, \lambda_\varkappa \quad i = 1, 2, \ldots, \mu$$

einsetzen, so wird der Ausdruck $\bar{Q}$ nur die Veränderlichen $y_{\lambda_{r+1}}, y_{\lambda_{r+2}}, \ldots, y_{\lambda_\varkappa}$ enthalten. Dieser Ausdruck sei mit Q^* bezeichnet. Wir zeigen jetzt, daß Q^* eine Konstante ist. Es gilt nämlich

$$(6) \qquad \frac{\partial Q^*}{\partial y_{\lambda_s}} = \sum_{i=1}^{\varkappa} \frac{\partial \bar{Q}}{dy_{\lambda_i}} \frac{\partial y_{\lambda_i}}{dy_{\lambda_s}} \qquad s = r+1, \; r+2, \ldots, \varkappa.$$

Aber dem linearen Gleichungssystem

$$\frac{\partial \bar{Q}}{\partial y_{\lambda_i}} = 0 \qquad i = 1, 2, \ldots, \varkappa,$$

also dem Gleichungssystem (4), genügt jedes solche Wertsystem y_{λ_i}, für welches die Werte $y_{\lambda_{r+1}}, y_{\lambda_{r+2}}, \ldots, y_{\lambda_\varkappa}$ beliebig und die $y_{\lambda_1}, y_{\lambda_2}, \ldots, y_{\lambda_r}$ nach (5) gewählt werden. Infolge-

dessen wird nach (6)

$$\frac{\partial Q^*}{\partial y_{\lambda_s}} = 0 \qquad\qquad s = r+1, \ldots, \varkappa,$$

w. z. b. w. Unser bisheriges Ergebnis ist also das folgende: *Wenn die Diskriminante der quadratischen Form einen verschwindenden Hauptminor besitzt, kann die Anzahl der Minimumstellen von $\overline{Q}$ unendlich sein*[6]*, die dazu gehörigen Minimumwerte sind jedoch dann alle untereinander gleich.* Wenn solche Minimumstellen existieren, dann liegt noch die Frage vor, ob es unter diesen Minimumstellen eine solche gibt, welche nicht negative Koordinaten besitzt, mit anderen Worten, ob das System von Ungleichungen

$$\begin{aligned}
&b_1 + c_{11}\, y_{\lambda_{r+1}} + c_{12}\, y_{\lambda_{r+2}} + \cdots + c_{1,\varkappa-r}\, y_{\lambda_\varkappa} \geqq 0\\
&b_2 + c_{21}\, y_{\lambda_{r+1}} + c_{22}\, y_{\lambda_{r+2}} + \cdots + c_{2,\varkappa-r}\, y_{\lambda_\varkappa} \geqq 0\\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots\\
&b_r + c_{r1}\, y_{\lambda_{r+1}} + c_{r2}\, y_{\lambda_{r+2}} + \cdots + c_{r,\varkappa-r}\, y_{\lambda_\varkappa} \geqq 0\\
&\qquad y_{\lambda_{r+1}} \qquad\qquad\qquad\qquad\qquad\qquad \geqq 0\\
&\qquad\qquad y_{\lambda_{r+2}} \qquad\qquad\qquad\qquad\qquad \geqq 0\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \qquad \vdots\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad y_{\lambda_\varkappa} \geqq 0
\end{aligned}$$

eine Lösung zuläßt. Die Theorie der linearen Ungleichungen wurde von H. Minkowski[7], J. Farkas[8] und neuerdings von A. Haar[9] entwickelt. L. L. Dines[10] hat in einer wichtigen Arbeit den Begriff „*Ungleichungsrang*" eingeführt. Mit Hilfe dieses Begriffes kann man entscheiden ob ein lineares Ungleichungssystem eine Lösung besitzt oder nicht. Der „Ungleichungsrang" wird für die Matrix eines Systems linearer Ungleichungen durch sukzessive Bildung weiterer Matrizen festgelegt. Also kann man bloß mit Hilfe der Koeffizienten des Systems über die Existenz der Lösung entscheiden. Wenn das System eine Lösung besitzt und die quadratische Form relativ definit positiv ist, soll der gemeinsame Minimumwert, welchen der quadratische Ausdruck Q in den unter (5) gegebenen unendlich vielen Punkten annimmt, positiv sein. Es ist hinreichend dies nur für einen solchen Punkt zu prüfen, z. B. für den Punkt

$$y_{\lambda_1} = b_1, \quad y_{\lambda_1} = b_2, \ldots, y_{\lambda_r} = b_r, \quad y_{\lambda_{r+1}} = y_{\lambda_{r+2}} = \cdots = y_{\lambda_n} = 0.$$

4. Wir wollen endlich denjenigen Fall erwähnen, in welchem unter den Gleichungssystemen (4) sich kein solches befindet, welches eine nicht negative Lösung besitzt. In diesem Falle werden die für $\mu = n-2$, $\nu = 1$ aus (4) folgenden Gleichungen

$$a_{\lambda_1 \lambda_1}\, y_{\lambda_1} = -\, a_{\lambda_1 r_1} \qquad 1 \leqq \lambda_1 \leqq n,\ 1 \leqq r_1 \leqq n$$

eine negative Lösung haben. Dies ist aber trivialerweise hinreichend dafür, daß die quadratische Form für positive Werte der Veränderlichen positiv sei.

---

[6]) Dies wird eintreffen, wenn: 1. das Gleichungssystem (4) auflösbar ist, 2. die Determinante des Gleichungssystems (4) die Diskriminante einer positiv definiten oder positiv semidefiniten qu. Form ist.

[7]) H. Minkowski, Geometrie der Zahlen, S. 39—45.

[8]) J. Farkas, Theorie der einfachen Ungleichungen, dieses Journal **124** (1901), S. 1—27.

[9]) A. Haar, Über lineare Ungleichungen, Acta Szeged **2** (1924-1926), S. 1—14.

[10]) L. L. Dines, Systems of linear inequalities, Annals of Mathematics **20** (1918—1919), S. 191—199.

Szeged, den 1. Dezember 1929.

Eingegangen 8. März 1930.

Über die Darstellung endlicher Abelscher Gruppen durch Kollineationen.

Von *Robert Frucht* in Triest.

Einleitung.

Aus der von Herrn I. Schur [1]) entwickelten Theorie der Darstellungen einer endlichen Gruppe durch gebrochene lineare Substitutionen seien zunächst die für das Folgende wichtigsten Resultate angeführt (vgl. D., Einleitung):

Ordnet man den Elementen $A, B, \ldots$ einer endlichen Gruppe $\mathfrak{G}$ der Ordnung g die g (nicht notwendig verschiedenen) f-reihigen Matrizen (A), (B), ... mit nicht verschwindenden Determinanten zu, so bilden diese eine *Darstellung des Grades* f [2]) von $\mathfrak{G}$ durch Kollineationen, wenn für je zwei Elemente A, B der Gruppe eine Gleichung

$$(1) \qquad (A)\,(B) = r_{A,B}\,(AB)$$

besteht, wo $r_{A,B}$ eine Konstante bedeutet. *Äquivalenz* und *Irreduzibilität* [3]) von Darstellungen werden wie bei ganzen linearen Substitutionen [4]) definiert. *Assoziiert* heißen zwei Darstellungen durch Kollineationen mit den Matrizen (A), (B), ... und (A'), (B'), ..., wenn es g Zahlen $a, b, \ldots$ gibt, so daß

$$(2) \qquad (A') = a(A), \qquad (B') = b(B), \ldots$$

wird. Da bei Kollineationen ein Zahlenfaktor keine Rolle spielt, sieht man zwei Darstellungen einer Gruppe durch Kollineationen nur dann als *wesentlich verschieden* an, wenn es keine zu der ersten assoziierte Darstellung gibt, die der zweiten äquivalent ist. Enthält eine endliche Gruppe $\mathfrak{H}$ eine aus invarianten Elementen von $\mathfrak{H}$ bestehende Untergruppe $\mathfrak{J}$ derart, daß die Faktorgruppe $\frac{\mathfrak{H}}{\mathfrak{J}}$ der Gruppe $\mathfrak{G}$ einstufig isomorph ist, so liefert jede i. Dg. [5]) von $\mathfrak{H}$ durch g. l. S. [5]) eine i. Dg. von $\mathfrak{G}$ durch Kollineationen, indem man einem Element A aus $\mathfrak{G}$ diejenige Matrix (A) zuordnet, die irgendeinem Element aus der A beim Isomorphismus entsprechenden Nebengruppe $\mathfrak{J}A$ bei der Darstellung von $\mathfrak{H}$ zugeordnet ist. $\mathfrak{H}$ läßt sich dabei so wählen, daß man alle wesentlich verschiedenen i. Dgn. von $\mathfrak{G}$ durch Kollineationen erhält (eventuell einige mehrfach), wenn man alle i. Dgn. von $\mathfrak{H}$ durch g. l. S. betrachtet. Dann heißt $\mathfrak{H}$ eine *hinreichend ergänzte Gruppe* von $\mathfrak{G}$; und speziell, wenn die Ordnung von $\mathfrak{H}$ möglichst klein gewählt

---

[1]) Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, dieses Journal Bd. **127** (1904), S. 20—50; Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, dieses Journal Bd. **132** (1907), S. 85—137. *Diese Arbeiten werden mit* D. *bzw.* U. *zitiert.*

[2]) Ist $f = 1$, so sprechen wir von einer *trivialen Darstellung.*

[3]) Herr Schur gebracht für *irreduzibel* noch die ältere Bezeichnung *primitiv.*

[4]) Vgl. z. B. A. Speiser, Die Theorie der Gruppen von endlicher Ordnung, 2. Aufl., Berlin 1927. *Fortan mit* Sp. *zitiert.*

[5]) Fortan werden folgende *Abkürzungen* benutzt: i. Dg(n). = irreduzible Darstellung(en), g. l. S. = ganze lineare Substitutionen.

wird, eine *Darstellungsgruppe* von $\mathfrak{G}$; in diesem Falle nennt man die als abstrakte Gruppe eindeutig bestimmte Gruppe $\mathfrak{J}$ den *Multiplikator* von $\mathfrak{G}$ [6]). Eine hinreichend ergänzte Gruppe $\mathfrak{K}$ von $\mathfrak{G}$ ist dann und nur dann eine Darstellungsgruppe, wenn der Kommutator [7]) $\mathfrak{K}^*$ von $\mathfrak{K}$ alle Elemente von $\mathfrak{J}$ enthält. Eine Gruppe, deren Multiplikator die Ordnung 1 hat, heißt eine *abgeschlossene* Gruppe.

Für Abelsche Gruppen hat Herr Schur gezeigt (U., VIII):

Sind $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ die Ordnungen der Elemente einer Basis der Abelschen Gruppe $\mathfrak{A}$, so ist der Multiplikator von $\mathfrak{A}$ das direkte Produkt von $\binom{n}{2}$ zyklischen Gruppen der Ordnungen $(\varepsilon_1, \varepsilon_2), (\varepsilon_1, \varepsilon_3), \ldots, (\varepsilon_{n-1}, \varepsilon_n)$. Zyklische Gruppen sind abgeschlossen [8]).

In der vorliegenden Arbeit sollen nun für Abelsche Gruppen die Darstellungen durch Kollineationen und die Darstellungsgruppen untersucht werden. Als Hauptresultat wird sich eine genaue Bestimmung der Anzahl der voneinander wesentlich verschiedenen i. Dgn. einer Abelschen Gruppe durch Kollineationen ergeben. Für eine beliebige Gruppe $\mathfrak{G}$ weiß man nämlich nur folgendes: Bedeutet k die Anzahl von Klassen konjugierter Elemente in einer Darstellungsgruppe $\mathfrak{K}$ von $\mathfrak{G}$, so gibt es genau k wesentlich verschiedene (d. h. nicht äquivalente) i. Dgn. von $\mathfrak{K}$ durch g. l. S., also höchstens ebensoviel [9]) verschiedene i. Dgn. von $\mathfrak{G}$ durch Kollineationen. Bezeichnet s die Anzahl der wesentlich verschiedenen i. Dgn. von $\mathfrak{G}$ durch Kollineationen, so kann man demnach nur

$$s \leqq k \tag{3}$$

behaupten. Bezeichnet ferner m die Ordnung des Multiplikators $\mathfrak{M}$ von $\mathfrak{G}$, so ist

$$s \geqq m; \tag{4}$$

denn zwei i. Dgn. von $\mathfrak{K}$, die zu verschiedenen Charakteren der Untergruppe $\mathfrak{M}$ gehören, führen stets auf wesentlich verschiedene Kollineationen (D., § 1.)

Bei Abelschen Gruppen wird sich nun durch Aufstellung einer Darstellungsgruppe (§ 1) und Untersuchung ihrer i. Dgn. durch g. l. S. (§ 2) ergeben (§ 3): *Die Anzahl der wesentlich verschiedenen i. Dgn. einer Abelschen Gruppe durch Kollineationen ist genau gleich der Ordnung ihres Multiplikators* [10]).

Dabei wird außerdem bewiesen werden (§ 3): *Ist f der Grad einer i. Dg. der Abelschen Gruppe $\mathfrak{A}$ durch Kollineationen, so geht das Quadrat von f in der Ordnung von $\mathfrak{A}$ auf* [11]).

Dann soll die Frage untersucht werden, welche Abelschen Gruppen eine *einstufig isomorphe* Darstellung als irreduzible Kollineationsgruppe zulassen; als notwendige und hinreichende Bedingung erweist sich, daß die Abelsche Gruppe als direktes Produkt zweier Abelscher Gruppen vom gleichen Typus geschrieben werden kann (§ 4). Ein rechnerisches Verfahren, um alle i. Dgn. einer Abelschen Gruppe durch Kollineationen

---

[6]) Auch der Kommutator jeder Darstellungsgruppe ist als abstrakte Gruppe allein durch $\mathfrak{G}$ eindeutig bestimmt, während eine Gruppe $\mathfrak{G}$ mehrere Darstellungsgruppen haben kann.

[7]) Wir bezeichnen den Kommutator einer Gruppe $\mathfrak{G}$ stets mit $\mathfrak{G}^*$.

[8]) Neuerdings hat Herr H. Weyl (Gruppentheorie und Quantenmechanik, Leipzig 1928, S. 148) die Frage nach den Darstellungen einer Abelschen Gruppe durch Kollineationen aufgeworfen, doch wird außer den zyklischen Gruppen nur die Vierergruppe als Beispiel behandelt.

[9]) Es kann nämlich bei zwei nicht äquivalenten i. Dgn. von $\mathfrak{K}$, wenn man sie als i. Dgn. von $\mathfrak{G}$ durch Kollineationen deutet, eine assoziierte der einen der anderen äquivalent sein, so daß beide als Kollineationen nicht wesentlich verschieden sind.

[10]) Bei allen anderen Gruppen ist hingegen $s > m$.

[11]) Für beliebige Gruppen stimmt das nicht, wie die Diedergruppen von nicht durch 4 teilbarer Ordnung zeigen, die eine i. Dg. vom Grade 2 besitzen; allgemein gilt nur, daß der Grad selber in der Ordnung der Gruppe aufgeht (D., § 4).

wirklich aufzustellen, wird in § 5 angegeben, dagegen die Anzahl der i. Dgn. eines bestimmten Grades nur für den Typus $(p, p, \ldots, p)$ bestimmt (§ 6).

In § 7 wird gezeigt, daß die Darstellungsgruppen einer Abelschen Gruppe, die metabelsche Gruppen sind (§ 1), auch noch metabelsche Darstellungsgruppen haben. In dem speziellen Fall, daß die Abelsche Gruppe direktes Produkt zweier zyklischer Gruppen (aber nicht selber zyklisch) ist, gibt es unter den Darstellungsgruppen auch abgeschlossene, die aber im wesentlichen schon von Herrn Schur als Beispiele abgeschlossener Gruppen angegeben worden sind.

§ 1. Die einfachste Darstellungsgruppe einer Abelschen Gruppe.

I. *Ist* $\mathfrak{H}$ *eine Darstellungsgruppe der Abelschen Gruppe* $\mathfrak{A}$, *so ist der Kommutator* $\mathfrak{H}^*$ *gleichzeitig der Multiplikator von* $\mathfrak{A}$.

Denn der Multiplikator $\mathfrak{M}$ von $\mathfrak{A}$ enthält als invariante Untergruppe von $\mathfrak{H}$ mit Abelscher Faktorgruppe $\frac{\mathfrak{H}}{\mathfrak{M}}$ den Kommutator $\mathfrak{H}^*$. Andererseits enthält bei einer beliebigen Gruppe der Kommutator $\mathfrak{H}^*$ einer Darstellungsgruppe den Multiplikator $\mathfrak{M}$ (Einl.).

Nennt man Gruppen mit Abelscher Kommutatorgruppe (wie üblich) *metabelsch*, so folgt aus I:

II. *Die Darstellungsgruppen Abelscher Gruppen sind metabelsche Gruppen.*

Eine hinreichend ergänzte Gruppe läßt sich nach folgendem auf beliebige Gruppen anwendbaren Verfahren bilden (U., S. 105, S. 106 Anm.): Die durch n Elemente $A_1, A_2, \ldots, A_n$ der Ordnungen $a_1, a_2, \ldots, a_n$ erzeugte Gruppe $\mathfrak{G}$ sei durch ein System [12])

$$f_\varkappa(A_1, A_2, \ldots, A_n) = E \qquad (\varkappa = 1, 2, \ldots, q)$$

von q Relationen zusammen mit den Ordnungsrelationen

$$A_\nu^{a_\nu} = E \qquad (\nu = 1, 2, \ldots, n)$$

völlig definiert; dann erhält man eine hinreichend ergänzte Gruppe $\mathfrak{R}$ von $\mathfrak{G}$ durch folgende Festsetzungen: In $\mathfrak{R} = (\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n)$ sei

$$\mathrm{A}_\nu^{a_\nu} = \mathrm{E} \qquad (\nu = 1, 2, \ldots, n),$$

ferner sollen die q Elemente $\mathrm{J}_\varkappa = f_\varkappa(\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n)$ invariante Elemente der Gruppe $\mathfrak{R}$ sein. Definiert man noch $\mathfrak{J} = \{\mathrm{J}_1, \mathrm{J}_2, \ldots, \mathrm{J}_q\}$, so ist $\frac{\mathfrak{R}}{\mathfrak{J}} \sim \mathfrak{G}$ [13]), und zwar entspricht dem Potenzprodukt $g(A_1, \ldots, A_n)$ in $\mathfrak{G}$ die Nebengruppe $\mathfrak{J} \cdot g(\mathrm{A}_1, \ldots, \mathrm{A}_n)$.

Um mit möglichst wenig erzeugenden Elementen auszukommen, schreibe man die zu betrachtende Abelsche Gruppe $\mathfrak{A}$ als direktes Produkt von n zyklischen Gruppen, wo die Ordnung einer jeden durch die der folgenden teilbar ist [14]):

$$\mathfrak{A} = \{A_1\} \times \{A_2\} \times \cdots \times \{A_n\}, \tag{5}$$

$$A_\nu^{a_\nu} = E \qquad (\nu = 1, 2, \ldots, n), \tag{6}$$

$$a_\nu \mid a_{\nu-1} \qquad (\nu = 2, 3, \ldots, n). \tag{7}$$

Da $\mathfrak{A}$ durch (6) und durch die $\binom{n}{2}$ Vertauschbarkeitsbedingungen

---

[12]) Dabei bedeutet $f_\varkappa(A_1, A_2, \ldots, A_n)$ ein gewisses Produkt von positiven oder negativen Potenzen der erzeugenden Elemente A_ν.

[13]) Das Zeichen $\sim$ bedeutet hier und im folgenden *einstufig isomorph*.

[14]) Hierbei kann $n > 1$ vorausgesetzt werden, da zyklische Gruppen abgeschlossen sind. Die (durch die Gruppe $\mathfrak{A}$ eindeutig festgelegten) Zahlen $a_1, a_2, \ldots, a_n$ heißen wie üblich die *Invarianten* der Abelschen Gruppe und $\mathfrak{A}$ vom *Typus* $(a_1, a_2, \ldots, a_n)$.

(8) $$A_\varkappa^{-1} A_\lambda^{-1} A_\varkappa A_\lambda = E \qquad (\varkappa < \lambda;\ \varkappa, \lambda = 1, 2, \ldots, n)$$

definiert ist, erhält man eine hinreichend ergänzte Gruppe $\mathfrak{H}$ von $\mathfrak{A}$ durch folgende Festsetzungen: In $\mathfrak{H} = (A_1, A_2, \ldots, A_n)$ sei

(9) $$A_\nu^{a_\nu} = E \qquad (\nu = 1, 2, \ldots, n),$$

und die $\binom{n}{2}$ Elemente

(10) $$C_{\varkappa\lambda} = A_\varkappa^{-1} A_\lambda^{-1} A_\varkappa A_\lambda \qquad (\varkappa < \lambda;\ \varkappa, \lambda = 1, 2, \ldots, n),$$

die die Gruppe $\mathfrak{J}$ erzeugen, sollen invariante Elemente sein. Hier ist aber $\mathfrak{J} = \mathfrak{H}^*$, und da $\mathfrak{J} < \mathfrak{H}^*$ das Kriterium dafür ist (Einl.), daß eine hinreichend ergänzte Gruppe Darstellungsgruppe ist, ist $\mathfrak{H}$ eine Darstellungsgruppe und nach I. $\mathfrak{H}^*$ der Multiplikator von $\mathfrak{A}$:

III. *Die durch* (9) *und* (10) *definierte Gruppe* $\mathfrak{H}$ *ist eine Darstellungsgruppe von* $\mathfrak{A}$, *die die „einfachste Darstellungsgruppe" heißen möge* [15]).

Erhebt man die aus (10) hervorgehende Gleichung $C_{\varkappa\lambda} A_\lambda^{-1} = A_\varkappa^{-1} A_\lambda^{-1} A_\varkappa$ in die a_λ-te Potenz, so ergibt sich wegen (9):

(11) $$C_{\varkappa\lambda}^{a_\lambda} = E.$$

Wir behaupten nun: $C_{\varkappa\lambda}$ ist von der genauen Ordnung a_λ, und zwischen $C_{12}, C_{13}, \ldots, C_{n-1,n}$ besteht sonst keine Relation. Zum Beweis greifen wir ein beliebiges festes Indexpaar $\varkappa < \lambda$ heraus und geben eine Darstellung von $\mathfrak{H}$ durch g. l. S. an, bei der $C_{\varkappa\lambda}$ von der genauen Ordnung a_λ ist, alle übrigen $C_{\varrho\sigma}$ aber durch die Einheitsmatrix dargestellt werden. Eine solche Darstellung wird durch folgende monomiale Substitutionen in a_λ Variablen $x_1, x_2, \ldots, x_{a_\lambda}$ geliefert, wo $\varepsilon_\varkappa$ eine primitive $a_\varkappa$-te Einheitswurzel bedeutet:

$$(A_\varkappa) = \begin{pmatrix} x_\varrho \\ \varepsilon_\varkappa^{-\left(1+\varrho\frac{a_\varkappa}{a_\lambda}\right)} x_\varrho \end{pmatrix} \qquad (\varrho = 1, 2, \ldots, a_\lambda),$$

(12) $$(A_\lambda) = \begin{pmatrix} x_1 x_2 \ldots x_{a_\lambda - 1} x_{a_\lambda} \\ x_2 x_3 \ldots x_{a_\lambda} \quad x_1 \end{pmatrix},$$

$(A_\mu) = (E)$, wenn μ ein von $\varkappa$ und λ verschiedener Index aus der Reihe $1, 2, \ldots, n$ ist.

Es wird dann

$$(C_{\varkappa\lambda}) = \varepsilon_\varkappa^{\frac{a_\varkappa}{a_\lambda}}(E)$$

tatsächlich invariantes Element von der genauen Ordnung a_λ und $(C_{\mu\nu}) = (E)$, wenn μ, ν von $\varkappa, \lambda$ verschieden ist.

Unser Ergebnis läßt sich auch so aussprechen (in Übereinstimmung mit U., VIII):

IV. *Der Multiplikator* $\mathfrak{H}^* = \{C_{12}\} \times \{C_{13}\} \times \{C_{23}\} \times \{C_{14}\} \times \cdots \times \{C_{n-1,n}\}$ *ist vom Typus* $(a_2, a_3, a_3, a_4, a_4, a_4, \ldots, \underbrace{a_n, a_n, \ldots, a_n}_{(n-1)\text{-mal}})$.

Die Ordnung von $\mathfrak{H}^*$ *ist daher*

(13) $$h^* = a_2\, a_3^2\, a_4^3 \cdots a_n^{n-1},$$

diejenige von $\mathfrak{H}$

(14) $$h = a_1\, a_2^2\, a_3^3 \cdots a_n^n.$$

Beispiel: Die einfachste Darstellungsgruppe der Vierergruppe ($a_1 = a_2 = 2$) ist die Diedergruppe der Ordnung 8.

---

[15]) $\mathfrak{H}$ ist keineswegs die einzige Darstellungsgruppe von $\mathfrak{A}$ (vgl. § 7); es ist sogar möglich, daß man bei verschiedener Wahl der erzeugenden Elemente $A_1, A_2, \ldots, A_n$ in $\mathfrak{A}$ auf formal verschiedene „einfachste Darstellungsgruppen" geführt wird.

§ 2. Die Darstellung von $\mathfrak{H}$ durch ganze lineare Substitutionen.

Man sagt von einer i. Dg. der Gruppe $\mathfrak{H}$ durch g. l. S., sie *entspreche* dem Charakter $\psi(C)$ von $\mathfrak{H}^*$, wenn das Element C von $\mathfrak{H}^*$ durch $\psi(C) \cdot (E)$ dargestellt wird. Wir nennen eine solche i. Dg. auch kürzer eine Darstellung Γ_ψ; bezeichnen wir ihre Matrizen durch Klammern, so ist für je zwei Elemente A, B aus $\mathfrak{H}$:

$$(A)(B)(A)^{-1}(B)^{-1} = \psi(ABA^{-1}B^{-1}) \cdot (E). \tag{15}$$

Bei festem A möge nun B alle Elemente von $\mathfrak{H}$ durchlaufen. Dann sind zwei Fälle möglich:

1. $\psi(ABA^{-1}B^{-1}) = 1$ oder $(A)(B)(A)^{-1}(B)^{-1} = (E)$ für alle B; dann ist (A) als eine mit allen Matrizen einer irreduziblen Substitutionsgruppe vertauschbare Matrix eine *Multiplikation*, d. h. von der Form $c \cdot (E)$ [16];

2. Es gibt ein Element B in $\mathfrak{H}$, so daß $\psi(ABA^{-1}B^{-1}) \neq 1$ oder $(A)(B)(A)^{-1}(B)^{-1} \neq (E)$ ist; dann ist (A) keine Multiplikation. In diesem Falle folgt durch rechtsseitige Multiplikation von (15) mit $(B)(A)(B)^{-1}$ und Übergang zu den Spuren, weil ähnliche Matrizen dieselbe Spur haben:

$$\chi(A) = \psi(ABA^{-1}B^{-1}) \cdot \chi(A) \quad \text{oder}$$
$$\chi(A) = 0. \tag{16}$$

Da bei einem Element A zur Entscheidung, welcher der beiden Fälle vorliegt, gar nicht die Kenntnis von Γ_ψ, sondern nur die des Charakters $\psi(C)$ von $\mathfrak{H}^*$ erforderlich ist und da offenbar die Gesamtheit der Multiplikationen eine $\mathfrak{H}^*$ enthaltende invariante Untergruppe liefert, hat sich ergeben:

V. *Diejenigen Elemente* $A < \mathfrak{H}$, *die bei einer i. Dg.* Γ_ψ *durch eine Multiplikation dargestellt werden, bilden eine (nur durch* $\psi(C)$ *bestimmte, von der speziellen Wahl der i. Dg.* Γ_ψ *unabhängige) invariante Untergruppe* $\mathfrak{U}_\psi$. *Zu* $\mathfrak{U}_\psi$ *gehören diejenigen Elemente* A, *für die die Gleichung*

$$\psi(AHA^{-1}H^{-1}) = 1 \tag{17}$$

für alle H *erfüllt ist. Die (und nur die) Elemente* B, *die nicht in* $\mathfrak{U}_\psi$ *liegen, haben bei* Γ_ψ *den Charakter* $\chi(B) = 0$.

Daher ist, wenn unsere i. Dg. Γ_ψ den Grad f_ψ hat:

$$\chi(H)\,\overline{\chi}(H) = \begin{cases} f_\psi^2, & \text{wenn } H < \mathfrak{U}_\psi, \\ 0, & \text{wenn H nicht in } \mathfrak{U}_\psi, \end{cases}$$

und die Fundamentalformel (Sp., S. 169) $\sum_H \chi(H)\,\overline{\chi}(H) = h$ lehrt, daß die Ordnung von $\mathfrak{U}_\psi$ gleich $\frac{h}{f_\psi^2}$ ist:

VI. *Der Grad* f_ψ *einer i. Dg.* Γ_ψ *ist gleich der Quadratwurzel aus dem Index von* $\mathfrak{U}_\psi$ *in bezug auf* $\mathfrak{H}$.

Für die Anzahl l_ψ der nicht äquivalenten i. Dgn. von $\mathfrak{H}$ durch g. l. S., die dem Charakter $\psi(C)$ von $\mathfrak{H}^*$ entsprechen, folgt daraus, da die Quadratsumme ihrer Grade nach einer Formel von Frobenius (D., Gleichung 21) gleich der Ordnung $\prod_{\nu=1}^{n} a_\nu$ von $\mathfrak{A}$ sein muß:

$$l_\psi f_\psi^2 = a_1 a_2 \cdots a_n . \tag{18}$$

Daraus ergibt sich wegen VI:

VII. *Die Anzahl* l_ψ *der nicht äquivalenten i. Dgn. von* $\mathfrak{H}$, *die dem Charakter* $\psi(C)$ *von* $\mathfrak{H}^*$ *entsprechen, ist gleich der Ordnung der Faktorgruppe* $\frac{\mathfrak{U}_\psi}{\mathfrak{H}^*}$.

---

[16]) Sp., Satz 149.

§ 3. Die Darstellungen von $\mathfrak{A}$ durch Kollineationen.

Eine Darstellung einer Gruppe durch Kollineationen heiße eine *getreue*, wenn bei ihr zwei verschiedene Elemente der Gruppe durch zwei verschiedene Kollineationen, d. h. durch Matrizen, die sich nicht nur durch einen Zahlenfaktor unterscheiden, dargestellt werden [17]). Bei einer getreuen Darstellung wird demnach nur das Einheitselement durch eine Multiplikation dargestellt.

Deuten wird jetzt eine i. Dg. Γ_ψ als i. Dg. von $\mathfrak{A}$ durch Kollineationen, so werden nach V. und VII. gerade die l_ψ Elemente von $\frac{\mathfrak{U}_\psi}{\mathfrak{H}^*}$ durch Multiplikationen dargestellt. Daraus ergeben sich die beiden folgenden Sätze:

VIII. *Soll eine Abelsche Gruppe $\mathfrak{A}$ eine getreue i. Dg. durch Kollineationen besitzen, so muß $\mathfrak{H}^*$ mindestens einen Charakter $\psi(C)$ besitzen, für den $\mathfrak{U}_\psi = \mathfrak{H}^*$, mithin $l_\psi = 1$ wird* [18]).

IX. *Eine dem Charakter $\psi(C)$ von $\mathfrak{H}^*$ entsprechende i. Dg. von $\mathfrak{A}$ durch Kollineationen ist eine getreue i. Dg. derjenigen Faktorgruppe von $\mathfrak{A}$, die beim Isomorphismus $\frac{\mathfrak{H}}{\mathfrak{H}^*} \sim \mathfrak{A}$ der Faktorgruppe $\frac{\mathfrak{H}}{\mathfrak{U}_\psi}$ entspricht.*

Nach IX. sind alle l_ψ i. Dgn. von $\mathfrak{H}$ durch g. l. S., die einem Charakter $\psi(C)$ von $\mathfrak{H}^*$ entsprechen, getreue i. Dgn. der Abelschen Gruppe $\frac{\mathfrak{H}}{\mathfrak{U}_\psi}$ durch Kollineationen; es gibt aber überhaupt *nur eine* solche getreue i. Dg. von $\frac{\mathfrak{H}}{\mathfrak{U}_\psi}$, wie man erkennt, wenn man VIII. nicht auf $\mathfrak{A}$, sondern auf $\frac{\mathfrak{H}}{\mathfrak{U}_\psi}$ anwendet. Damit ist gezeigt:

X. *Die l_ψ einem Charakter $\psi(C)$ von $\mathfrak{H}^*$ entsprechenden i. Dgn. von $\mathfrak{H}$ durch g. l. S. sind, als i. Dgn. von $\mathfrak{A}$ durch Kollineationen aufgefaßt, nicht wesentlich voneinander verschieden.*

Da zwei verschiedenen Charakteren des Multiplikators entsprechende i. Dgn. durch Kollineationen immer wesentlich verschieden sind (Einl.), so ist die Anzahl der verschiedenen i. Dgn. von $\mathfrak{A}$ durch Kollineationen gleich der Anzahl der Charaktere von $\mathfrak{H}^*$. Damit ist der schon in der Einleitung angeführte Hauptsatz bewiesen [19]):

XI. *Die Anzahl der wesentlich verschiedenen i. Dgn. einer Abelschen Gruppe durch Kollineationen ist genau gleich der Ordnung ihres Multiplikators* [20]).

Für den Grad einer solchen i. Dg. folgt aus (18):

XII. *Ist f der Grad einer i. Dg. der Abelschen Gruppe $\mathfrak{A}$ durch Kollineationen, so geht f^2 in der Ordnung von $\mathfrak{A}$ auf. Der Grad der dem Charakter $\psi(C)$ von $\mathfrak{H}^*$ entprechenden i. Dg. von $\mathfrak{A}$ ist*

$$f_\psi = \sqrt{\frac{a_1\, a_2 \cdots a_n}{l_\psi}}. \tag{19}$$

---

[17] Diese Definition besagt, daß bei einer getreuen Darstellung zwischen abstrakter Gruppe und Kollineationsgruppe einstufiger Isomorphismus besteht.

[18]) Für welche Abelschen Gruppen das zutrifft, wird später (§ 4) untersucht werden.

[19]) Der Beweis wurde nur für $n \geqq 2$ geführt, doch gilt der Satz auch für zyklische Gruppen, da diese nur eine triviale Darstellung zulassen.

[20]) Die Abelschen Gruppen sind die einzigen, bei denen diese Anzahl s gleich der Ordnung des Multiplikators ist; bei allen anderen Gruppen ist $s > m$. Denn dem Hauptcharakter $\psi(M) = 1$ des Multiplikators einer nicht Abelschen Gruppe $\mathfrak{G}$ entsprechen alle diejenigen i. Dgn. einer Darstellungsgruppe, die gleichzeitig i. Dgn. von $\mathfrak{G}$ durch g. l. S. sind. Darunter kommt neben der trivialen Darstellung auch eine i.Dg. von höherem als dem ersten

Speziell für den Grad einer getreuen i. Dg. von $\mathfrak{A}$, die nach VIII. durch $l_\psi = 1$ charakterisiert ist, ergibt sich

$$f = \sqrt{a_1\, a_2 \cdots a_n}\,. \tag{20}$$

Daraus folgt: *Ist eine irreduzible Kollineationsgruppe vom Grade f Abelsch, so ist sie von der Ordnung f^2.*

§ 4. Berechnung von l_ψ. Die Bedingungen für die Existenz getreuer Darstellungen.

Für den Kommutator zweier Elemente aus $\mathfrak{H}$ gilt, wie man durch Ausrechnen bestätigt (oder U., S. 115 entnehmen kann):

$$(\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n})(\mathrm{A}_1^{\beta_1}\mathrm{A}_2^{\beta_2}\cdots\mathrm{A}_n^{\beta_n})(\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n})^{-1}(\mathrm{A}_1^{\beta_1}\mathrm{A}_2^{\beta_2}\cdots\mathrm{A}_n^{\beta_n})^{-1} = \prod_{\varkappa<\lambda}\mathrm{C}_{\varkappa\lambda}^{\left|\begin{smallmatrix}\alpha_\varkappa & \alpha_\lambda\\ \beta_\varkappa & \beta_\lambda\end{smallmatrix}\right|}. \tag{21}$$

Nach V. und VII. ist nun l_ψ wegen (22) $\mathfrak{H} = \sum_{\alpha_1,\ldots,\alpha_n} \mathfrak{H}^*\,\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n}$ gleich der Anzahl der Elemente von der Form $\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n}$, für die

$$\psi((\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n})\,\mathrm{H}(\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n})^{-1}\,\mathrm{H}^{-1}) = 1$$

für alle H oder wegen (21)

$$\prod_{\varkappa<\lambda}\psi(\mathrm{C}_{\varkappa\lambda})^{\alpha_\varkappa\beta_\lambda-\alpha_\lambda\beta_\varkappa} = 1 \tag{23}$$

für alle Werte der β_ν erfüllt ist.

Da $\mathrm{C}_{\varkappa\lambda}$ von der Ordnung a_λ ist (§ 1), erhält man wegen (7) einen Charakter $\psi(\mathrm{C})$ von $\mathfrak{H}^*$, wenn man eine primitive a_2-te Einheitswurzel ε bestimmt und

$$\psi(\mathrm{C}_{\varkappa\lambda}) = \varepsilon^{\frac{a_2}{a_\lambda}s_{\varkappa\lambda}} \qquad (\varkappa<\lambda;\ \varkappa,\lambda = 1,2,\ldots,n) \tag{24}$$

setzt [21]). Dann geht (23) über in $\prod_{\varkappa<\lambda}\varepsilon^{\frac{a_2}{a_\lambda}s_{\varkappa\lambda}(\alpha_\varkappa\beta_\lambda-\alpha_\lambda\beta_\varkappa)} = 1$ oder

$$\sum_{\varkappa<\lambda}\frac{a_2}{a_\lambda}s_{\varkappa\lambda}(\alpha_\varkappa\beta_\lambda-\alpha_\lambda\beta_\varkappa) \equiv 0 \pmod{a_2}. \tag{25}$$

Indem man die linke Seite in zwei Summen zerlegt und in der zweiten die Summationsbuchstaben vertauscht, ergibt sich

$$\sum_{\varkappa<\lambda}\frac{a_2}{a_\lambda}s_{\varkappa\lambda}\alpha_\varkappa\beta_\lambda - \sum_{\varkappa>\lambda}\frac{a_2}{a_\varkappa}s_{\lambda\varkappa}\alpha_\varkappa\beta_\lambda \equiv 0 \pmod{a_2},$$

oder wenn für $\varkappa \geqq \lambda$

$$s_{\varkappa\lambda} = -s_{\lambda\varkappa} \tag{26}$$

definiert wird:

$$\sum_{\varkappa=1}^{n}\sum_{\lambda=1}^{n}\frac{a_2\,s_{\varkappa\lambda}}{(a_\varkappa,a_\lambda)}\alpha_\varkappa\beta_\lambda \equiv 0 \pmod{a_2}. \tag{27}$$

Nun war l_ψ die Anzahl derjenigen $\mathrm{A}_1^{\alpha_1}\mathrm{A}_2^{\alpha_2}\cdots\mathrm{A}_n^{\alpha_n}$, für die (23) bei allen Werten der β_ν erfüllt ist. Also ist zu verlangen, daß die Kongruenz (27) für alle Werte von $\beta_1, \beta_2, \ldots, \beta_n$ gilt oder daß die n Kongruenzen

$$\sum_{\varkappa=1}^{n}\frac{a_2\,s_{\varkappa\nu}}{(a_\varkappa,a_\nu)}\alpha_\varkappa \equiv 0 \pmod{a_2} \tag{28}$$

Grade vor, und diese ist, auch als Kollineation aufgefaßt, von der trivialen wesentlich verschieden. Daher gehören schon zum Hauptcharakter mindestens zwei wesentlich verschiedene i. Dgn. von $\mathfrak{G}$ durch Kollineationen, also ist $s > m$.

[21]) Man erhält alle Charaktere von $\mathfrak{H}^*$, wenn jede der Größen $s_{\varkappa\lambda}$ ein vollständiges Restsystem mod. a_λ durchläuft.

erfüllt sind: l_ν ist gleich der Anzahl der simultanen Lösungen der n Kongruenzen (28) für die Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$, wobei α_ν aus einem vollständigen Restsystem mod. a_ν zu nehmen ist. Die Koeffizientenmatrix von (28), die

$$A = \left(\frac{a_2\, s_{\lambda\varkappa}}{(a_\varkappa, a_\lambda)}\right) \tag{29}$$

heißen möge, ist wegen (26) schiefsymmetrisch (alternierend) und möge die Elementarteiler $e_1, e_2, \ldots, e_n$ haben; d. h. es gibt zwei Matrizen U und V mit der Determinante ± 1, so daß

$$UAV = \begin{pmatrix} e_1 & 0 \cdots 0 \\ 0 & e_2 \cdots 0 \\ \cdots\cdots\cdots \\ 0 & 0 \cdots e_n \end{pmatrix} \tag{30}$$

wird, wobei

$$e_\mu \mid e_{\mu+1} \qquad (\mu = 1, 2, \ldots, n-1) \tag{31}$$

ist. Da A schiefsymmetrisch ist, ist [22])

$$e_1 = e_2, \quad e_3 = e_4, \ldots, \tag{32}$$

und falls n ungerade ist, $e_n = 0$.

Bezeichnet man die Zahlenreihe $\alpha_1, \alpha_2, \ldots, \alpha_n$ kurz mit α, so kann man die Kongruenzen (28) kürzer schreiben in der Form:

$$A(\alpha) \equiv 0 \pmod{a_2}. \tag{28a}$$

Führt man durch die unimodulare Substitution

$$\alpha = V(\xi), \quad \xi = V^{-1}(\alpha) \tag{33}$$

eine neue Zahlenreihe $\xi_1, \xi_2, \ldots, \xi_n$ ein, so bekommt man für die ξ_ν die Kongruenzen $AV(\xi) \equiv 0 \pmod{a_2}$ oder damit gleichbedeutend $UAV(\xi) \equiv 0 \pmod{a_2}$, d. h. wegen (30):

$$e_\nu \xi_\nu \equiv 0 \pmod{a_2} \qquad (\nu = 1, 2, \ldots, n). \tag{34}$$

Die allgemeine Lösung dieser Kongruenzen ist

$$\xi_\nu = \frac{a_2}{(a_2, e_\nu)} t_\nu \qquad (\nu = 1, 2, \ldots, n), \tag{35}$$

wo die Parameter $t_1, t_2, \ldots, t_n$ alle ganzen Zahlen durchlaufen sollen, also nach (33) die von (28a):

$$\alpha_\mu = \sum_{\nu=1}^{n} v_{\mu\nu} t_\nu \frac{a_2}{(a_2, e_\nu)} \qquad (\mu = 1, 2, \ldots, n), \tag{36}$$

wo die $v_{\varkappa\lambda}$ die Elemente der Matrix V bedeuten. Oder anders ausgedrückt unter Einführung von n Symbolen $x_1, x_2, \ldots, x_n$: Die Lösungen von (28a) bilden einen n-gliedrigen Modul $\mathfrak{m}$ von Linearformen $\sum_{\mu=1}^{n} \alpha_\mu x_\mu$, der als Basis die n Formen

$$\sum_{\mu=1}^{n} v_{\mu\nu} \frac{a_2}{(a_2, e_\nu)} x_\mu \qquad (\nu = 1, 2, \ldots, n)$$

hat mit der Koeffizientenmatrix

---

[22]) Siehe Frobenius, Theorie der linearen Formen mit ganzen Coeffizienten, dieses Journal Bd. 86 (1879), S. 167.

$$(37) \qquad M = \left(v_{\lambda\varkappa}\frac{a_2}{(a_2, e_\varkappa)}\right) = \begin{pmatrix} \frac{a_2}{(a_2, e_1)} & 0 & \cdots & 0 \\ 0 & \frac{a_2}{(a_2, e_2)} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \frac{a_2}{(a_2, e_n)} \end{pmatrix} \cdot V' .$$

Als Anzahl der Lösungen von (28a), wenn $\alpha_\nu \pmod{a_\nu}$ reduziert wird ($\nu = 1, 2, \ldots, n$), ist daher l_ψ gleich der Anzahl der Restklassen, in die der Modul $\mathfrak{m}$ zerfällt nach demjenigen n-gliedrigen Teilmodul $\mathfrak{a}$, der als Basis die n Linearformen

$$(38) \qquad a_1 x_1, a_2 x_2, \ldots, a_n x_n$$

hat, also gleich dem absoluten Betrag des Quotienten aus den Determinanten der Koeffizientenmatrizen von (38) und (37):

$$l_\psi = \pm \frac{a_1 a_2 \cdots a_n}{|M|}$$

oder wegen $|V| = \pm 1$

$$(39) \qquad l_\psi = \frac{\prod_{\nu=1}^{n} a_\nu \cdot \prod_{\nu=1}^{n} (a_2, e_\nu)}{a_2^n} .$$

Für den Grad f_ψ einer dem Charakter $\psi(C)$ von $\mathfrak{H}^*$ entsprechenden i. Dg. folgt daraus nach (19) und (32)

$$(40) \qquad f_\psi = \frac{a_2^{\left[\frac{n}{2}\right]}}{(a_2, e_2)\,(a_2, e_4)\,(a_2, e_6)\cdots(a_2, e_{2\left[\frac{n}{2}\right]})} .$$

Jetzt läßt sich auch die Frage beantworten, wann eine Abelsche Gruppe getreue i. Dgn. durch Kollineationen besitzt. Dazu ist nach VIII. notwendig und hinreichend die Existenz eines Charakters $\psi(C)$ von $\mathfrak{H}^*$, für den $l_\psi = 1$, also $\mathfrak{m} = \mathfrak{a}$ wird. Dann muß die Matrix M in (37) dieselben Elementarteiler haben wie die Matrix $\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$ von (38). So erhalten wir die Bedingungen: $\frac{a_2}{(a_2, e_\nu)} = a_\nu$ oder

$$(41) \qquad (a_2, e_\nu) = \frac{a_2}{a_\nu} \qquad (\nu = 1,2, \ldots, n) .$$

Im Falle eines ungeraden n führt die n-te dieser Bedingungen wegen $e_n = 0$ auf den Widerspruch $a_n = 1$. Infolgedessen muß n gerade sein. Weiter ergibt sich aus (41) wegen (32) als notwendige Bedingung für die Existenz getreuer i. Dgn. bei geradem n:

$$(42) \qquad a_1 = a_2, \; a_3 = a_4, \ldots, a_{n-1} = a_n .$$

Diese Bedingungen sind aber auch hinreichend; denn wählt man speziell als Charakter $\psi(C)$ von $\mathfrak{H}^*$ denjenigen, bei dem

$$(43) \qquad s_{12} = s_{34} = \cdots = s_{n-1,n} = 1, \; s_{21} = s_{43} = \cdots = s_{n,n-1} = -1$$

ist und alle übrigen $s_{\varrho\sigma} = 0$ sind, so wird tatsächlich $l_\psi = 1$. Damit ist gezeigt:

XIII. *Dafür, daß die Abelsche Gruppe $\mathfrak{A}$ getreue i. Dgn. durch Kollineationen besitzt (oder: daß $\mathfrak{A}$ einer irreduziblen Kollineationsgruppe einstufig isomorph ist), ist not-*

wendig und hinreichend, daß n gerade und $a_1 = a_2, a_3 = a_4, \ldots, a_{n-1} = a_n$ ist, d. h. daß $\mathfrak{A}$ als direktes Produkt zweier Abelscher Gruppen von gleichem Typus geschrieben werden kann.

§ 5. Ein Verfahren zur Bestimmung aller Darstellungen.

Es sei zunächst $\mathfrak{A}$ eine Abelsche Gruppe mit geradem n und paarweise gleichen Invarianten:

$$a_1 = a_2, \quad a_3 = a_4, \ldots, a_{n-1} = a_n . \tag{42}$$

Der bisher mit $\psi(C)$ bezeichnete, durch (24) gegebene Charakter von $\mathfrak{H}^*$ heiße jetzt genauer $\psi_{C_{12}^{s_{12}} C_{13}^{s_{13}} \ldots C_{n-1,n}^{s_{n-1,n}}}(C)$. [23]) Das Wesentliche an der neuen Bezeichnung ist, daß die Charaktere bei der Komposition eine zu $\mathfrak{H}^*$ isomorphe Gruppe bilden, z. B. ist

$$\psi_{C_{12}}(C) \cdot \psi_{C_{34}}(C) \cdot \psi_{C_{56}}(C) \cdots \psi_{C_{n-1,n}}(C) = \psi_{C_{12} C_{34} C_{56} \cdots C_{n-1,n}}(C) . \tag{44}$$

Bereits in § 1 haben wir in (12) eine Darstellung von $\mathfrak{H}$ durch g. l. S. des Grades a_λ kennen gelernt. Setzt man für die dortige primitive $a_\varkappa$-te Einheitswurzel: $\varepsilon_\varkappa = \varepsilon^{\frac{a_2}{a_\varkappa} c_\lambda}$ mit $(c_\lambda, a_\varkappa) = 1$, wo ε unsere primitive a_2-te Einheitswurzel bedeutet, so entspricht diese Darstellung, die $\Gamma_{\varkappa\lambda}^{(c_\lambda)}$ heißen möge, dem Charakter $\psi_{C_{\varkappa\lambda}^{c_\lambda}}(C)$ von $\mathfrak{H}^*$. Man bilde nun die durch *Komposition* [24]) aus $\Gamma_{12}^{(1)}, \Gamma_{34}^{(1)}, \ldots, \Gamma_{n-1,n}^{(1)}$ entstehende Darstellung $\Gamma_{12}^{(1)} \times \Gamma_{34}^{(1)} \times \cdots \times \Gamma_{n-1,n}^{(1)}$; sie ist vom Grade $f = a_2 a_4 a_6 \cdots a_n$ und entspricht nach (44) dem Charakter $\psi_{C_{12} C_{34} \cdots C_{n-1,n}}(C)$ von $\mathfrak{H}^*$. Sie ist irreduzibel; denn wäre sie reduzibel, so würde ein irreduzibler Bestandteil einen Grad haben, der kleiner ist als $a_2 a_4 a_6 \cdots a_n$, was nicht geht, da hier wegen $l_\psi = 1$ der Grad einer i. Dg. nach (20) genau $a_2 a_4 a_6 \cdots a_n$ sein muß. Entsprechend erhält man in $\Gamma_{12}^{(c_2)} \times \Gamma_{34}^{(c_4)} \times \cdots \times \Gamma_{n-1,n}^{(c_n)}$ eine getreue i. Dg., die dem Charakter $\psi_{C_{12}^{c_2} C_{34}^{c_4} \ldots C_{n-1,n}^{c_n}}(C)$ entspricht, wenn für $\nu = 2, 4, \ldots, n$

$$(c_\nu, a_\nu) = 1 \text{ ist.} \tag{45}$$

Auf diesen Fall läßt sich aber der Fall eines beliebigen Charakters $\psi_{C_{12}^{s_{12}} C_{13}^{s_{13}} \ldots C_{1n}^{s_{1n}} C_{23}^{s_{23}} \ldots C_{n-1,n}^{s_{n-1,n}}}(C)$ von $\mathfrak{H}^*$, für den $l_\psi = 1$ ist, durch einen geeigneten Automorphismus von $\mathfrak{H}$ zurückführen und dadurch die Aufgabe lösen, *alle* getreuen i. Dgn. von $\mathfrak{A}$ durch Kollineationen anzugeben. Sind nämlich $e_1 = e_2, e_3 = e_4, \ldots, e_{n-1} = e_n$ die wegen $l_\psi = 1$ den Bedingungen (41) $(a_2, e_\nu) = \frac{a_2}{a_\nu}$ genügenden Elementarteiler der Matrix (29) $A = \left(\frac{a_2 s_{\lambda\varkappa}}{(a_\varkappa, a_\lambda)}\right)$, so gibt es nach einem Satz von Frobenius [25]) eine Matrix $\Omega = (\omega_{\varkappa\lambda})$ mit $|\Omega| = 1$, so daß

$$A = \Omega' \cdot \begin{pmatrix} 0 & e_2 & 0 & 0 & \cdots & 0 & 0 \\ -e_2 & 0 & 0 & 0 & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & e_4 & \cdots & \cdots & \cdots \\ 0 & 0 & -e_4 & 0 & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 & e_n & \\ 0 & \cdots & 0 & \cdots & -e_n & 0 & \end{pmatrix} \cdot \Omega \tag{46}$$

---

[23]) Der durch (43) definierte Charakter z. B. wäre jetzt als $\psi_{C_{12} C_{34} C_{56} \cdots C_{n-1,n}}(C)$ zu bezeichnen.

[24]) Siehe z. B. Sp., § 53.

[25]) Siehe Frobenius, a. a. O., S. 167 f.

oder

$$(47)\qquad \frac{a_2\, s_{\varkappa\lambda}}{(a_\varkappa, a_\lambda)} = -\, e_2 \begin{vmatrix} \omega_{1\varkappa} & \omega_{1\lambda} \\ \omega_{2\varkappa} & \omega_{2\lambda} \end{vmatrix} - e_4 \begin{vmatrix} \omega_{3\varkappa} & \omega_{3\lambda} \\ \omega_{4\varkappa} & \omega_{4\lambda} \end{vmatrix} - \cdots - e_n \begin{vmatrix} \omega_{n-1,\varkappa} & \omega_{n-1,\lambda} \\ \omega_{n\varkappa} & \omega_{n\lambda} \end{vmatrix} \qquad (\varkappa, \lambda = 1,2, \ldots, n)$$

wird. Wir betrachten den durch

$$(48)\qquad \mathrm{A}_\nu = \overline{\mathrm{A}}_1^{\omega_{1\nu}} \overline{\mathrm{A}}_2^{\omega_{2\nu}} \cdots \overline{\mathrm{A}}_n^{\omega_{n\nu}} \qquad (\nu = 1, 2, \ldots, n)$$

definierten Automorphismus [26]) von $\mathfrak{H}$ und in den transformierten Elementen den Charakter $\psi_{\overline{\mathrm{C}}_{12}^{c_2} \overline{\mathrm{C}}_{34}^{c_4} \cdots \overline{\mathrm{C}}_{n-1,n}^{c_n}}(\mathrm{C})$ von $\mathfrak{H}^*$, wo $\overline{\mathrm{C}}_{\varkappa\lambda} = \overline{\mathrm{A}}_\varkappa^{-1} \overline{\mathrm{A}}_\lambda^{-1} \overline{\mathrm{A}}_\varkappa \overline{\mathrm{A}}_\lambda$ $(\varkappa < \lambda)$ und

$$(49)\qquad c_\nu = -\frac{e_\nu}{(a_2, e_\nu)} = -\frac{e_\nu a_\nu}{a_2} \qquad (\nu = 2, 4, \ldots, n)$$

gesetzt ist, und wegen (41) die Bedingungen (45) erfüllt sind. Nach (21) wird:

$$(50)\qquad \mathrm{C}_{\varkappa\lambda} = \prod_{\varrho<\sigma} \overline{\mathrm{C}}_{\varrho\sigma}^{\begin{vmatrix} \omega_{\varrho\varkappa} & \omega_{\varrho\lambda} \\ \omega_{\sigma\varkappa} & \omega_{\sigma\lambda} \end{vmatrix}} \qquad (\varkappa < \lambda;\ \varkappa, \lambda = 1, 2, \ldots n),$$

$$\psi_{\overline{\mathrm{C}}_{12}^{c_2} \overline{\mathrm{C}}_{34}^{c_4} \cdots \overline{\mathrm{C}}_{n-1,n}^{c_n}}(\mathrm{C}_{\varkappa\lambda}) = \prod_{\varrho<\sigma} \psi_{\overline{\mathrm{C}}_{12}^{c_2} \overline{\mathrm{C}}_{34}^{c_4} \cdots \overline{\mathrm{C}}_{n-1,n}^{c_n}}(\overline{\mathrm{C}}_{\varrho\sigma})^{\begin{vmatrix} \omega_{\varrho\varkappa} & \omega_{\varrho\lambda} \\ \omega_{\sigma\varkappa} & \omega_{\sigma\lambda} \end{vmatrix}},$$

und wenn man (49) und die Definition von $\psi_{\overline{\mathrm{C}}_{12}^{c_2} \overline{\mathrm{C}}_{34}^{c_4} \cdots \overline{\mathrm{C}}_{n-1,n}^{c_n}}(\overline{\mathrm{C}})$ berücksichtigt, die für die Elemente $\overline{\mathrm{C}}_{12}, \overline{\mathrm{C}}_{34}, \ldots$ die Charaktere $\varepsilon^{c_2} = \varepsilon^{-e_2}$, $\varepsilon^{\frac{a_2}{a_4} c_4} = \varepsilon^{-e_4}, \ldots$, für $\overline{\mathrm{C}}_{13}, \overline{\mathrm{C}}_{14}, \ldots$ aber 1 als Charakter liefert,

$$\psi_{\overline{\mathrm{C}}_{12}^{c_2} \overline{\mathrm{C}}_{34}^{c_4} \cdots \overline{\mathrm{C}}_{n-1,n}^{c_n}}(\mathrm{C}_{\varkappa\lambda}) = \varepsilon^{-e_2 \begin{vmatrix} \omega_{1\varkappa} & \omega_{1\lambda} \\ \omega_{2\varkappa} & \omega_{2\lambda} \end{vmatrix} - e_4 \begin{vmatrix} \omega_{3\varkappa} & \omega_{3\lambda} \\ \omega_{4\varkappa} & \omega_{4\lambda} \end{vmatrix} - \cdots - e_n \begin{vmatrix} \omega_{n-1,\varkappa} & \omega_{n-1,\lambda} \\ \omega_{n\varkappa} & \omega_{n\lambda} \end{vmatrix}} = \varepsilon^{\frac{a_2}{a_\lambda} s_{\varkappa\lambda}}$$

für $\varkappa < \lambda$ nach (47), folglich

$$(51)\qquad \psi_{\mathrm{C}_{12}^{s_{12}} \mathrm{C}_{13}^{s_{13}} \cdots \mathrm{C}_{n-1,n}^{s_{n-1,n}}}(\mathrm{C}_{\varkappa\lambda}) = \psi_{\overline{\mathrm{C}}_{12}^{c_2} \overline{\mathrm{C}}_{34}^{c_4} \cdots \overline{\mathrm{C}}_{n-1,n}^{c_n}}(\mathrm{C}_{\varkappa\lambda}).$$

Durch den Automorphismus erscheint also jeder Charakter mit $l_\psi = 1$ auf den bereits behandelten Spezialfall zurückgeführt und damit das Problem, alle getreuen i. Dgn. von $\mathfrak{A}$ durch Kollineationen aufzustellen, gelöst.

Ist jetzt $\mathfrak{A}$ wieder eine beliebige Abelsche Gruppe, so ist nach IX. eine i. Dg. von von $\mathfrak{A}$ durch Kollineationen getreue i. Dg. einer Faktorgruppe von $\mathfrak{A}$, die nach XIII. paarweise gleiche Invarianten aufweisen muß. Da soeben ein Verfahren angegeben wurde, alle getreuen i. Dgn. einer solchen Abelschen Gruppe aufzustellen, so ist damit auch die Aufgabe gelöst, alle i. Dgn. einer Abelschen Gruppe zu bestimmen:

XIV. *Um alle i. Dgn. einer Abelschen Gruppe $\mathfrak{A}$ durch Kollineationen aufzustellen, suche man in $\mathfrak{A}$ alle diejenigen Faktorgruppen auf, die lauter paarweise einander gleiche Invarianten besitzen, und bestimme für jede derselben nach dem in diesem Paragraphen dargelegten Verfahren sämtliche getreue i. Dgn. durch Kollineationen* [27]).

Im Fall $n = 2$ sind alle diese Faktorgruppen von der Form $\frac{\mathfrak{A}}{\{A_1^d, A_2^d\}}$ mit $d \mid a_2$. Man findet so als eine dem Charakter $\psi(\mathrm{C}_{12}) = \varepsilon^{s_{12}}$ entsprechende i. Dg. von $\mathfrak{A}$ für $s_{12} = 1, 2, \ldots a_2 - 1$ [28]):

[26]) Daß (48) tatsächlich ein Automorphismus ist, rechnet man leicht nach.

[27]) Um die triviale Darstellung von $\mathfrak{A}$ nicht auszuschließen, muß man auch $\frac{\mathfrak{A}}{\mathfrak{A}}$ zu diesen Faktorgruppen rechnen, obwohl man dabei nicht gut von paarweise gleichen Invarianten sprechen kann.

[28]) Dem Fall $s_{12} = 0$ entspricht ja die triviale Darstellung.

$$(52)\qquad \left.\begin{aligned}(A_1) &= \begin{pmatrix} x_1 & x_2 & x_3 & \dots x_d \\ \varepsilon^{-s_{12}} x_1 & \varepsilon^{-2s_{12}} x_2 & \varepsilon^{-3s_{12}} x_3 & \dots x_d \end{pmatrix} \\ (A_2) &= \begin{pmatrix} x_1 & x_2 & x_3 \dots x_{d-1} & x_d \\ x_2 & x_3 & x_4 \dots x_d & x_1 \end{pmatrix}\end{aligned}\right\} \qquad d = \frac{a_2}{(a_2, s_{12})}.$$

(52) ist eine getreue i. Dg. von $\dfrac{\mathfrak{A}}{\{A_1^d, A_2^d\}}$ mit $d = \dfrac{a_2}{(a_2, s_{12})}$; die Anzahl der verschiedenen i. Dgn. von einem bestimmten Grade $f \mid a_2$ beträgt demnach $\varphi(f)$. Hingegen findet man für die Anzahl l_ψ der einem Charakter $\psi(C_{12}) = \varepsilon^{s_{12}}$ entsprechenden verschiedenen i. Dgn. von $\mathfrak{H}$ durch g. l. S. nach (39) $l_\psi = \dfrac{a_1}{a_2}(a_2, s_{12})^2$ und somit für die Anzahl von Klassen konjugierter Elemente in $\mathfrak{H}$:

$$(53)\qquad k = \sum_\psi l_\psi = \frac{a_1}{a_2} \sum_{s_{12}=0}^{a_2-1} (a_2, s_{12})^2 = \frac{a_1}{a_2} \sum_{\delta \mid a_2} \delta^2 \varphi\left(\frac{a_2}{\delta}\right)^{29}).$$

§ 6. $\mathfrak{A}$ vom Typus $(p, p, \dots, p)$.

Für den Fall, daß (54) $a_1 = a_2 = \cdots = a_n = p$ (Primzahl) und (55) $n = 2l$ eine gerade Zahl ist, möge noch die Anzahl $Z(p, n, l)$ der *getreuen* i. Dgn. durch Kollineationen bestimmt werden. Bei einer getreuen i. Dg. muß $l_\psi = 1$ oder nach (41)

$$(56)\qquad (e_\nu, p) = 1 \qquad (\nu = 1, 2, \dots, n)$$

sein, wo $e_1 = e_2, e_3 = e_4, \dots, e_{n-1} = e_n$ die Elementarteiler der Matrix $A = (-s_{\varkappa\lambda})$ sind; A muß also mod. p den Rang $n = 2l$ haben, wie man auch direkt den Kongruenzen (28) entnehmen kann. *$Z(p, n, l)$ ist infolgedessen gleich der Anzahl der mod. p verschiedenen alternierenden n-reihigen Matrizen mit nicht durch p teilbarer Determinante.*

Um $Z(p, n, l,)$ zu bestimmen, setzen wir

$$(57)\quad N = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 0 & 0 & 0 & \cdots & & \\ 0 & 0 & 0 & 1 & \cdots & & \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 \\ \cdots & & & & & & \\ 0 & \cdots & 0 & \cdots & & 0 & 1 \\ 0 & \cdots & 0 & \cdots & & -1 & 0 \end{pmatrix} \quad \text{und} \quad \Delta = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & e_2 & 0 & 0 & \cdots & & \\ 0 & 0 & 1 & 0 & \cdots & & \\ 0 & 0 & 0 & e_4 & \cdots & 0 & 0 \\ \cdots & & & & & & \\ 0 & \cdots & 0 & \cdots & & 1 & 0 \\ 0 & \cdots & 0 & \cdots & & 0 & e_n \end{pmatrix};$$

dann ist $|\Delta| \not\equiv 0 \pmod p$ wegen (56), und die aus (46) hervorgehende Gleichung $A = \Omega'\Delta' N \Delta\Omega = (\Delta\Omega)' N (\Delta\Omega)$ lehrt, daß man jede alternierende Matrix A mit nicht durch p teilbarer Determinante in der Form

$$(58)\qquad A \equiv \Lambda' N \Lambda \pmod p$$

schreiben kann, wo Λ eine Matrix mit $|\Lambda| \not\equiv 0 \pmod p$ ist. Alle mod. p verschiedenen alternierenden Matrizen mit nicht durch p teilbarer Determinante erhält man also in den verschiedenen unter den Matrizen $\Lambda' N \Lambda$, wenn man Λ die Gruppe $\mathfrak{L}_n$ aller g. l. S. mod. p in n Variablen mit nicht durch p teilbarer Determinante durchlaufen läßt, deren Ordnung [30])

---

[29]) Für $n > 2$ besteht eine so einfache Formel nicht mehr. — Wegen eines weiteren Beispiels sei auf die Arbeit von Herrn Schur: Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, dieses Journal Bd. **139** (1911), S. 155—250, verwiesen, wo in § 21 durch ein dem hier geschilderten ganz ähnliches Kompositionsverfahren für die Abelsche Gruppe der Ordnung 2^{2m} vom Typus $(2,2,\dots,2)$ die dem Charakter $\psi_{C_{12}C_{13}\cdots C_{1n}C_{23}\cdots C_{n-1,n}}(C)$ entsprechende getreue i. Dg. durch Kollineationen des Grades 2^m gebildet wird.

[30]) Sp., S. 129.

$$l_n = p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \tag{59}$$

ist.

Die Untergruppe $\mathfrak{B}_n$ derjenigen Substitutionen aus $\mathfrak{L}_n$, die bei kogredienter Anwendung auf die Variablenreihen $x_1, x_2, \ldots, x_{2l}$ und $y_1, y_2, \ldots, y_{2l}$ die zur Matrix N gehörige Bilinearform

$$(x_1 y_2 - x_2 y_1) + (x_3 y_4 - x_4 y_3) + \cdots + (x_{2l-1} y_{2l} - x_{2l} y_{2l-1})$$

mod. p invariant lassen, nennt man die spezielle lineare Abelsche Gruppe des $GF(p)$; ihre Ordnung ist [31])

$$b_n = p^{\frac{n^2}{4}} (p^2 - 1)(p^4 - 1) \cdots (p^{n-2} - 1)(p^n - 1). \tag{60}$$

Liefern nun zwei Substitutionen Λ_1 und Λ_2 dieselbe alternierende Matrix $\Lambda_1' N \Lambda_1 \equiv \Lambda_2' N \Lambda_2$ (mod. p), so ist $(\Lambda_1 \Lambda_2^{-1})' N (\Lambda_1 \Lambda_2^{-1}) \equiv N \pmod{p}$, $\Lambda_1 \Lambda_2^{-1} < \mathfrak{B}_n$, Λ_1 und Λ_2 gehören derselben rechtsseitigen Nebengruppe von $\mathfrak{L}_n$ mod. $\mathfrak{B}_n$ an. $Z(p, n, l)$ ist daher gleich dem Index von $\mathfrak{B}_n$ unter $\mathfrak{L}_n$:

$$Z(p, n, l) = \frac{l_n}{b_n} = p^{\frac{n}{2}\left(\frac{n}{2}-1\right)} (p^{n-1} - 1)(p^{n-3} - 1) \cdots (p^3 - 1)(p - 1). \tag{61}$$

Aus (61) läßt sich für eine Abelsche Gruppe mit $a_1 = a_2 = \cdots = a_n = p$ und mit beliebigem $n > 1$ die Anzahl $Z(p, n, \alpha)$ der verschiedenen i. Dgn. durch Kollineationen des Grades p^α berechnen. Wegen

$$Z(p, n, 0) = 1 \tag{62}$$

und XII. können wir uns auf $\alpha = 1, 2, \ldots, \left[\frac{n}{2}\right]$ beschränken. Nun ist nach IX. und (20) eine i. Dg. vom Grade p^α getreue i. Dg. einer Faktorgruppe von $\mathfrak{A}$, die die Ordnung $p^{2\alpha}$ hat. Die Anzahl der getreuen i. Dgn. einer solchen Faktorgruppe, die sich aus (61) ergibt, wenn man das dortige $n = 2l$ durch 2α ersetzt, ist nur noch, um $Z(p, n, \alpha)$ zu erhalten, mit der Anzahl der verschiedenen Faktorgruppen von der Ordnung $p^{2\alpha}$ in $\mathfrak{A}$ zu multiplizieren, also (Sp., Satz 51) mit

$$\frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-2\alpha+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^{2\alpha} - 1)};$$

so ergibt sich:

XV. *Die Anzahl der verschiedenen i. Dgn. durch Kollineationen des Grades p^α, die die Abelsche Gruppe vom Typus $(p, p, \ldots, p)$ mit der Ordnung p^n besitzt, beträgt* [32]):

$$Z(p, n, \alpha) = p^{\alpha(\alpha-1)} \frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-2\alpha+1} - 1)}{(p^2 - 1)(p^4 - 1) \cdots (p^{2\alpha} - 1)} \tag{63}$$

$$\left(\alpha = 1, 2, \ldots, \left[\frac{n}{2}\right];\quad n \geqq 2\right).$$

---

[31]) L. E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Leipzig 1901, S. 94.

[32]) Da $\mathfrak{A}$ nach XI. im ganzen $p^{\binom{n}{2}}$ verschiedene i. Dgn. durch Kollineationen besitzt, ist wegen (62)

$$\sum_{\alpha=1}^{\left[\frac{n}{2}\right]} Z(p, n, \alpha) = p^{\binom{n}{2}} - 1.$$

Dies läßt vermuten, daß auch für eine beliebige Größe x die Gleichung

$$x^{\binom{n}{2}} - 1 = \sum_{\alpha=1}^{\left[\frac{n}{2}\right]} x^{\alpha(\alpha-1)} \frac{(x^n - 1)(x^{n-1} - 1) \cdots (x^{n-2\alpha+1} - 1)}{(x^{2\alpha} - 1)(x^{2\alpha-2} - 1) \cdots (x^2 - 1)} \qquad (n = 2, 3, \ldots)$$

gilt; tatsächlich besteht eine solche Identität, wie man z. B. durch vollständige Induktion beweisen kann.

§ 7. Die Darstellungsgruppen einer Abelschen Gruppe.

Alle Darstellungsgruppen der Abelschen Gruppe $\mathfrak{A}$ vom Typus $(a_1, a_2, \ldots, a_n)$ erhält man nach dem von Herrn Schur für beliebige Gruppen angegebenen Verfahren (U., § 1, insbesondere S. 94 f.) in der Form $\mathfrak{H} = \{A_1, A_2, \ldots, A_n\}$, wenn man wieder die Forderung stellt, daß die $\binom{n}{2}$ Elemente

$$C_{\varkappa\lambda} = A_\varkappa^{-1} A_\lambda^{-1} A_\varkappa A_\lambda \qquad (\varkappa < \lambda;\ \varkappa, \lambda = 1, 2, \ldots, n) \tag{10}$$

invariante Elemente von $\mathfrak{H}$ sein sollen, aber die bisherigen Ordnungsrelationen (9) durch die allgemeineren Bedingungen

$$A_\mu^{a_\mu} = \prod_{\varkappa<\lambda} C_{\varkappa\lambda}^{\alpha_{\varkappa\lambda\mu}} \qquad (\mu = 1, 2, \ldots, n) \tag{64}$$

ersetzt, wobei jeder Exponent $\alpha_{\varkappa\lambda\mu}$ auf ein vollständiges Restsystem mod. (a_λ, a_μ) beschränkt werden darf.

Bemerkenswert ist, daß im Fall $n = 2$ die Darstellungsgruppe $\mathfrak{H}$ mit den Exponenten $\alpha_{121} = \alpha_{122} = 1$ eine abgeschlossene Gruppe ist. Da nämlich in diesem Falle

$$C_{12} = A_1^{a_1} = A_2^{a_2} \tag{65}$$

ist, so gilt in einer Darstellungsgruppe $\mathfrak{L} = \{\bar{A}_1, \bar{A}_2\}$ von $\mathfrak{H}$ für die entsprechenden, durch Überstreichung bezeichneten Elemente: $\bar{C}_{12} = M_1 \bar{A}_1^{a_1} = M_2 \bar{A}_2^{a_2}$, wo M_1 und M_2 als Elemente des Multiplikators $\mathfrak{M}$ von $\mathfrak{H}$ invariante Elemente sind. Daher ist $\bar{C}_{12}$ mit $\bar{A}_1$ und $\bar{A}_2$ vertauschbar, also invariantes Element von $\mathfrak{L}$, und folglich besteht der Kommutator $\mathfrak{L}^* = \{\mathfrak{M}, \bar{C}_{12}\}$ aus lauter invarianten Elementen. Aus $\frac{\mathfrak{L}}{\mathfrak{L}^*} \sim \mathfrak{A}$ folgt dann, daß $\mathfrak{L}$ eine durch die Gruppe $\mathfrak{L}^*$ ergänzte Gruppe von $\mathfrak{A}$ ist; die Ordnung einer Gruppe mit dieser Eigenschaft kann aber nicht größer als die von $\mathfrak{H}$ sein (D., S. 47).

Da hier (65) zur Definition von $\mathfrak{H}$ genügt — daß C_{12} invariantes Element ist, folgt daraus von selber —, ist also bewiesen, wenn man noch $a_1 = uv$, $a_2 = v$ setzt:

XVI. *Durch* $A^{u^v} = B^v = A^{-1} B^{-1} AB$ *ist eine abgeschlossene (und nicht zyklische) Gruppe der Ordnung* uv^3 *definiert.* $(u = 1, 2, \ldots;\ v = 2, 3, \ldots)$

Für $u = 1$, $v = 2$ z. B. ergibt sich die Quaternionengruppe. Wählt man $u = p^{\mu-2\nu}$, $v = p^\nu$, wo $\mu \geqq 2\nu$, wenn p eine von 2 verschiedene Primzahl, und $\mu > 2\nu$ bei $p = 2$ sein soll, so erhält man eine abgeschlossene Gruppe der Ordnung $p^{\mu+\nu}$, die mit der von Herrn Schur in U., S. 108 Anm. angegebenen isomorph ist. Um auf die dortige Definition zu kommen, hat man nur $A = P$ und $A^{-p^{\mu-2\nu}} \cdot B = Q$ zu setzen, wie man durch eine leichte Rechnung bestätigen kann.

Im allgemeinen haben jedoch die Darstellungsgruppen einer Abelschen Gruppe einen von E verschiedenen Multiplikator, dessen genaue Ordnung schwierig zu bestimmen ist. Hier soll nur noch folgender Satz bewiesen werden:

XVII. *Die Darstellungsgruppen einer Darstellungsgruppe einer Abelschen Gruppe sind wieder metabelsche Gruppen.*

Ist nämlich $\mathfrak{L}$ eine Darstellungsgruppe und $\mathfrak{M}$ der Multiplikator einer Darstellungsgruppe $\mathfrak{H}$, so folgt aus $\frac{\mathfrak{L}}{\mathfrak{M}} \sim \mathfrak{H}$ wegen $\mathfrak{M} < \mathfrak{L}^*$ auch $\frac{\mathfrak{L}^*}{\mathfrak{M}} \sim \mathfrak{H}^*$; also da für jedes Element $C < \mathfrak{H}^*$ und für jedes Element $A < \mathfrak{H}$ $CAC^{-1}A^{-1} = E$ ist, ist entsprechend für jedes Element $\bar{C} < \mathfrak{L}^*$ und $\bar{A} < \mathfrak{L}$, $\bar{C}\bar{A}\bar{C}^{-1}\bar{A}^{-1} = M_{\bar{A}}$ ein Element aus $\mathfrak{M}$. Aus $\bar{C}\bar{A}\bar{C}^{-1} = M_{\bar{A}}\bar{A}$ und $\bar{C}\bar{B}\bar{C}^{-1} = M_{\bar{B}}\bar{B}$ folgt aber durch Multiplikation $M_{\bar{A}\cdot\bar{B}} = M_{\bar{A}} \cdot M_{\bar{B}}$, also $M_{\bar{A}\bar{B}\bar{A}^{-1}\bar{B}^{-1}} = \bar{E}$ und überhaupt $M_{\bar{D}} = \bar{E}$ für $\bar{D} < \mathfrak{L}^*$. Damit ist aber $\bar{C}\bar{D}\bar{C}^{-1}\bar{D}^{-1} = \bar{E}$ für irgend zwei Elemente $\bar{C}$ und $\bar{D}$ aus $\mathfrak{L}^*$ bewiesen.

Eingegangen 14. März 1930.

Darstellung relativ Abelscher Zahlkörper durch Primkörper und Einheitskörper.

Von *F. Neiss* in Berlin-Charlottenburg.

Die vorliegende Arbeit soll eine Übersicht über sämtliche relativ Abelschen Zahlkörper geben, die sich über dem rationalen oder einem imaginär-quadratischen Grundkörper bilden lassen. Die Körper werden dabei nach ihrer Relativdiskriminante und nach ihrem Relativgrad geordnet. Im Gegensatz zur allgemeinen Klassenkörpertheorie werden hier wesentlich einfachere Hilfsmittel benutzt. Analytische Methoden der Zahlentheorie sind vermieden. Es handelt sich nur darum, arithmetische Grundlagen zum Beweis der Kroneckerschen Vollständigkeitssätze zu schaffen. Es ist daher nicht die Absicht, und wohl auch mit den hier gebrauchten Mitteln nicht möglich, die Existenz der betreffenden Körper nachzuweisen.

Der Inhalt läßt sich so zusammenfassen:

Es sei Γ_r ein relativ zyklischer Körper von Primzahlpotenzgrad $n = q^r$ über k, wir schreiben dafür Γ_r/k, und es sei k ein imaginärer quadratischer Körper:

$$k = R(\sqrt{-D}),$$

wo R den Bereich der rationalen Zahlen und D eine positive Zahl bedeutet. Es kann auch $k = R$ sein.

Es wird gezeigt, daß Γ_r als Teiler in einem Produkt von solchen, über k zyklischen Körpern vorkommen muß, deren Grad ebenfalls eine Potenz von q ist und deren Relativdiskriminante entweder eine Einheit ist, oder die Potenz von nur einem Primideal aus k ist. Außerdem wird festgestellt, wieviel verschiedene solcher Körper existieren können, oder genauer ausgedrückt: Wieviel Körper gibt es, deren Grad $n = q^r$ ist, und deren Relativdiskriminante eine Einheit oder eine Potenz von einem gegebenen Primideal aus k ist? Daraus ergibt sich eine Art eindeutiger Zerlegung des allgemeinen zyklischen Körpers in solche von einfacherer Beschaffenheit. Es mag daher gerechtfertigt sein, wenn ich statt der sonst üblichen Bezeichnungsweise „unverzweigte Körper" von einem „Einheitskörper" spreche, wenn die Relativdiskriminante eine Einheit ist, und von einem „Primkörper", wenn die Relativdiskriminante die Potenz von nur einem Primideal ist. (Zur genaueren Definition vergl. Satz 6 und Satz 15.)

In dieser Ausdrucksweise lautet der Satz, der hier bewiesen werden soll:

Alle relativ Abelschen Körper können dadurch eingefangen werden, daß man Primkörper und Einheitskörper multipliziert und die Teiler solcher Produkte aufsucht.

Der erste Teil behandelt den allgemeinen relativ zyklischen Körper von Primzahlpotenzgrad. Die Relativdiskriminante des allgemeinen Körpers wird von solchen Primidealen befreit, die zum Grad des Körpers teilerfremd sind. Der zweite Teil betrachtet nur solche Körper, deren Relativdiskriminante nur durch Ideale teilbar ist, die auch im Grad des Körpers aufgehen. Der dritte Teil behandelt die Einheitskörper.

Hier ist der Beweis nicht in voller Allgemeinheit durchgeführt, es ist nur der Fall erledigt, daß die Gruppe der Idealklassen des Grundkörpers zyklisch ist.

Wir wollen dabei noch den Fall ausschließen, daß der Grad eine Potenz von 2 ist. Während die im dritten Teil gemachte Einschränkung der Allgemeinheit notwendig war, weil die hier benutzten Mittel nicht beweiskräftig genug zu sein scheinen, um den Beweis allgemein durchzuführen, ist die letzte Maßnahme nur deshalb erfolgt, weil es aus äußeren Gründen zweckmäßig erschien, die Zahl 2 besonders zu behandeln.

Zusammenstellung der gebrauchten Bezeichnungen.

Es bedeutet:

R den Bereich der rationalen Zahlen,
D eine positive quadratfreie Zahl,
$k = R(\sqrt{-D})$ einen imaginär-quadratischen Körper,
q eine ungerade Primzahl,
$n = q^r$ eine Potenz von q,
ϱ_r eine primitive q^r-te Einheitswurzel (also $\varrho_v = \varrho_r^{q^{r-v}}$),
Γ_r einen relativ zyklischen Körper über k.

Der Relativgrad ist $n = q^r$, dabei ist r als Index angehängt, ferner ist unter Γ_v der Teiler q^v-ten Grades von Γ_r verstanden. Der Index bei ϱ ist überall dort weggelassen, wo ein Verwechseln einer q^r-ten mit einer q^r-ten Einheitswurzel nicht möglich ist. m ist der Relativgrad von $k(\varrho_r)$ in bezug auf k, also ist

$$\text{entweder } m = q^{r-1}(q-1) \quad \text{oder} \quad m = \tfrac{1}{2} q^{r-1}(q-1),$$

je nachdem k selbst im Körper der q-ten Einheitswurzeln enthalten ist oder nicht. Mit $l, l', l'', \ldots$ sind positive ganze Zahlen gemeint, die nicht durch q teilbar sind.

Ist k teilerfremd zu $R(\varrho)$, so bedeutet g eine Primitivwurzel von q^2; ist k in $R(\varrho)$ enthalten, so bezeichnet g das Quadrat einer solchen Primitivwurzel. Auf jeden Fall ist

$$g^m - 1 = nl.$$

$1, S, S^2, \ldots, S^{m-1}$ sind die Substitutionen der Gruppe des Körpers $k(\varrho_r)/k$.

Schließlich sei noch die Abkürzung

$$h(S) = 1 + S^{-1} g + S^{-2} g^2 + \cdots + S^{-(m-1)} g^{m-1}$$

erwähnt. Da $h(S)$ von r abhängt, so wird dies gelegentlich durch $h_r(S)$ angedeutet. Insbesondere ist

$$h_1(S) = \Sigma S^{-\nu} g^\nu \qquad \nu = 0, 1, \ldots, \quad q-1$$
$$\text{oder} \quad \nu = 0, 1, \ldots, \tfrac{1}{2}(q-1).$$

Außerdem wird im Ausdruck folgende Abkürzung gebraucht: Statt „Relativkörper“ „Relativgrad“, „Relativdiskriminante“ sagen wir einfach „Körper“, „Grad“, „Diskriminante“. Gemeint ist damit immer relativ zu k. Sollte gelegentlich auf einen anderen Grundkörper bezogen werden, so wird dies ausdrücklich bemerkt.

Erster Teil.

In meiner Arbeit über relativ Abelsche Zahlkörper (Sitzungsberichte der Berliner Mathematischen Gesellschaft, Mai 1920) ist gezeigt, daß alle zu $k(\varrho_r)$ teilerfremden, relativ zyklischen Körper Γ_r folgendermaßen erhalten werden: Man nehme eine Zahl $\varkappa$ aus $k(\varrho_r)$ und setze

(1) $$\omega = \varkappa^{h_r(S)}.$$

$\varkappa$ braucht nur der Forderung zu genügen, daß ω keine q-te Potenz einer Zahl aus $k(\varrho_r)$ ist; dann ist durch ω ein Körper Γ_r bestimmt, und es ist

$$k(\sqrt[n]{\omega}) = \Gamma_r \cdot k(\varrho_r)$$

Ist $r > 1$, so ist durch diese Zahl ω der Körper Γ_r nicht eindeutig festgelegt, da in dem Produkt $\Gamma_r(\varrho_r)$ mehrere zyklische Teiler q^r-ten Grades enthalten sind. Wir brauchen im ersten Teil diesen Umstand nicht zu beachten und sagen einfach: Γ_r/k sei durch ω bestimmt; gelegentlich wollen wir auch $\varkappa$ als die den Körper bestimmende Zahl bezeichnen, während $\sqrt[n]{\omega}$ die den Körper erzeugende Zahl ist.

ω kann durch $\omega^l \sigma^n$ ersetzt werden, wo σ eine beliebige von Null verschiedene Zahl aus $k(\varrho_r)$ bedeutet.

Die Funktion $h_r(S)$ hat folgende Eigenschaften:

$$(gS^{-1} - 1)\, h_r(S) = g^m - 1 = nl$$

oder

$$g\, h_r(S) \equiv S\, h_r(S) \pmod{n}.$$

Hieraus folgt für ein beliebiges $F(S)$:

$$(F(S) - F(g))\, h_r(S) \equiv 0 \pmod{n}. \tag{2}$$

Es sei ferner $m = ef$ irgendeine Zerlegung von m, und $h_r(S)$ stehe im Exponenten einer Zahl oder eines Ideals, das durch S^e ungeändert bleibt

$$z = z^{S^e}.$$

Dann kann in $z^{h_r(S)}$ schon $S^e = 1$ gesetzt werden, woraus sich für diesen besonderen Fall

$$\begin{aligned} h_r(S) &= (1 + g^e + g^{2e} + \cdots + g^{(f-1)e})\,(1 + gS^{-1} + g^2S^{-2} + \cdots + g^{e-1}S^{-(e-1)}) \\ &= \frac{g^m - 1}{g^e - 1} \sum_{\nu=0}^{e-1} g^\nu S^{-\nu} \end{aligned} \tag{3}$$

ergibt.

Aus (1) und (2) folgt:

$$\omega^{F(S)} = \omega^{F(g)} \sigma^n, \tag{4}$$

wo σ eine Zahl aus $k(\varrho_r)$ bezeichnet.

Hieraus ergibt sich:

Satz 1. Ist $F(g)$ nicht durch q teilbar, so kann ω durch $\omega^{F(S)}$ ersetzt werden. Mit anderen Worten: $F(S)$ und $F(g)$ sind als Exponenten von ω gleichwertig.

Gelegentlich hat man $\sqrt[q^a]{\omega}$ durch $\sqrt[q^{a+b}]{\omega^{q^b}}$ zu ersetzen. Dies kann so geschehen, daß man bei $\omega = \varkappa^{h_a(S)}$ von $h_a(S)$ zu $h_{a+b}(S)$ übergeht. Dann ist

$$\omega^{q^b} = \varkappa^{l h_{a+b}(S)}.$$

Dies ist richtig nach Gleichung (3), weil $\varkappa$ eine Zahl aus $k(\varrho_a)$ ist. Hieraus ergibt sich insbesondere: Ist ω_1 eine $h_a(S)$-te Potenz einer Zahl aus $k(\varrho_a)$, ω_2 eine $h_b(S)$-te Potenz einer Zahl aus $k(\varrho_b)$ und $b \leqq a$, so ist $\omega_1\, \omega_2^{q^{a-b}}$ jedenfalls eine $h_a(S)$-te Potenz.

Ist $\xi_1 = \sqrt[q^a]{\omega_1}$ und $\xi_2 = \sqrt[q^b]{\omega_2}$, so werden durch ξ_1 und ξ_2 zwei zyklische Körper Γ_a und Γ'_b erzeugt. Die Zahl

$$\eta = \xi_1^\alpha \xi_2^\beta$$

erzeugt für irgendwelche ganzzahligen α und β einen Teiler des Abelschen Körpers $k(\varrho_a, \xi_1, \xi_2)$. Auch der Körper $k(\varrho_a, \eta)$ läßt sich als Produkt eines zyklischen Körpers

q^ν-ten Grades Γ''_γ und $k(\varrho_a)$ auf verschiedene Arten darstellen. Wesentlich ist dabei, daß dieser durch η erzeugte Körper Γ''_γ immer so gewählt werden kann, daß er ein Teiler des Körpers $\Gamma_a\Gamma'_b/k$ wird. Man kann Γ''_γ eindeutig in der Weise festlegen, daß man ihn als den größten gemeinsamen Teiler von $\Gamma_a\Gamma'_b/k$ und $k(\eta, \varrho_a)$ definiert. Schließlich ergibt sich daraus, daß durch

$$\xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{r-1}}$$

der Reihe nach die Körper

$$\Gamma_r, \Gamma_{r-1}, \Gamma_{r-2}, \ldots, \Gamma_1$$

erzeugt werden. Dabei kann es auch vorkommen, daß die den Körper Γ_v bestimmende Zahl ω eine höhere als die ϱ_v-te Einheitswurzel enthält.

Wir fügen ohne Beweis noch folgenden Satz hinzu:

Satz 2. Haben zwei zyklische Körper Γ_a und Γ'_b einen gemeinsamen Teiler, so gibt es einen zyklischen Körper Γ''_c, so daß

$$\Gamma_a \cdot \Gamma'_b = \Gamma_a \cdot \Gamma''_c$$

und $c < b$ ist.

Satz 3. $\mathfrak{P}$ bezeichne ein zu q primes Primideal aus k und $\mathfrak{p}$ einen Teiler davon in $k(\varrho_r)$, so daß

$$\mathfrak{P} = \mathfrak{p}^{1+S+S^2+\cdots+S^{x-1}},$$

d. h. $\mathfrak{P}$ zerfalle in $k(\varrho_r)$ in x verschiedene zueinander konjugierte Primideale. Die Zerlegung von ω sei

$$(\omega) = \mathfrak{a} \cdot \mathfrak{p}^{q^\nu \varphi(S)},$$

wo $\mathfrak{a}$ zu $\mathfrak{P}$ teilerfremd ist und $\varphi(S)$ eine ganzzahlige Funktion von S bezeichnet, deren Koeffizienten nicht sämtlich durch q teilbar sind. Alsdann ist $\mathfrak{P}$ in der Diskriminante $\Delta_{\nu+1}$ von $\Gamma_{\nu+1}$ aber nicht in Δ_ν, der Diskriminante von Γ_ν, enthalten. Im Falle $\nu = 0$ sind $\Gamma_0 = k$ und $\Delta_0 = 1$ zu setzen. Ist $\nu = r$, so sagt der Satz nur aus, daß Δ_r zu $\mathfrak{P}$ prim ist.

Beweis: (vergl. Hilbert, Zahlbericht § 126).

Um Γ_ν darzustellen, kann ω durch

$$\omega' = \frac{\omega}{\sigma^{q^\nu}}$$

ersetzt werden. σ ist eine Zahl aus $k(\varrho_r)$, die genau durch $\mathfrak{p}^{\varphi(S)}$ teilbar ist. Die Diskriminante der Gleichung

$$x^{q^\nu} - \omega' = 0$$

ist zu $\mathfrak{p}, \mathfrak{p}^S, \ldots$ teilerfremd, also auch zu $\mathfrak{P}$. Um zu zeigen, daß $\Delta_{\nu+1}$ durch $\mathfrak{P}$ teilbar ist, setzen wir

$$\xi^{q^{\nu+1}} = \omega;$$

dann ist ξ eine Zahl aus $\Gamma_{\nu+1}(\varrho_r)$, und diese Gleichung zeigt, daß bei der Zerlegung eines der $\mathfrak{p}^{S^\nu}$ in dem Körper $k(\xi, \varrho_r)$ eine Verzweigung eintreten muß. Daher ist die Relativdiskriminante von $\Gamma_{\nu+1}(\varrho_r)$ über $k(\varrho_r)$ durch $\mathfrak{p}$ teilbar. Da die Zahlen aus $\Gamma_{\nu+1}$ bei der Substitution S ungeändert bleiben, so gehen auch alle zu $\mathfrak{p}$ konjugierten Ideale in dieser Relativdiskriminante auf, also auch $\mathfrak{P}$. Da es sich nur um die Teilbarkeit durch $\mathfrak{P}$, ein zu q primes Ideal, handelt, kommt es nicht darauf an, ob $\Gamma_{\nu+1}(\varrho_r)$ als Körper über $k(\varrho_r)$ oder $\Gamma_{\nu+1}$ über k betrachtet wird. Daher ist $\Delta_{\nu+1}$ durch $\mathfrak{P}$ teilbar.

Die folgenden Betrachtungen sollen weitere Bedingungen für die Teilbarkeit der Diskriminanten $\Delta_1, \ldots, \Delta_r$ durch ein zu q primes Primideal $\mathfrak{P}$ bringen. Dabei soll wie

vorher die Zahl v angeben, daß $\Delta_r, \ldots, \Delta_{v+1}$ durch $\mathfrak{P}$ teilbar, dagegen $\Delta_v, \ldots, \Delta_1$ zu $\mathfrak{P}$ teilerfremd sind.

Betrachten wir der Reihe nach die Zerlegung von $\mathfrak{P}$ in den Körpern $k(\varrho_1)$, $k(\varrho_2)\ldots$, so gibt es einen Körper $k(\varrho_z)$, so daß $\mathfrak{p}$, der Teiler von $\mathfrak{P}$ in $k(\varrho_z)$, vom ersten Relativgrade ist, d. h. alle zu $\mathfrak{p}$ konjugierten Ideale sind verschieden, während in $k(\varrho_{z+1})$ eine weitere Zerlegung von $\mathfrak{p}$ nicht mehr eintritt. Ist diese Bedingung schon in $k(\varrho_1)$ nicht erfüllt, so ist $z = 0$ zu setzen. Beiläufig sei bemerkt, daß $N(\mathfrak{P}) - 1$ genau durch q^z teilbar ist, wo $N(\mathfrak{P})$ die Norm von $\mathfrak{P}$ bezeichnet.

Satz 4. Damit $\mathfrak{P}$ Teiler von Δ_{v+1} sein kann, ist notwendig, daß $r - v \leqq z$ ist. (Vgl. Hilberts Zahlbericht Satz 21.)

Beweis: Ist schon $r \leqq z$, so sagt der Satz nichts aus. Wir nehmen daher $r \geqq z$. Es sei

$$\mathfrak{P} = \mathfrak{p}^{1+S+\cdots+S^{x-1}}$$

die Zerlegung von $\mathfrak{P}$ in $k(\varrho_r)$ und

$$\mathfrak{p}^{S^x} = \mathfrak{p}.$$

Wir greifen auf die Darstellung

$$\omega = \varkappa^{h_r(S)}$$

zurück und nehmen an, $\mathfrak{p}$ sei in $\varkappa$ in der Potenz $\psi(S)$ enthalten.

Setzt man wie vorher

$$(\omega) = \mathfrak{a} \cdot \mathfrak{p}^{q^v \varphi(S)},$$

so ist

$$q^v \varphi(S) = \psi(S)\, h_r(S).$$

Wir betrachten zunächst den Exponenten $h_r(S)$ und beachten, daß $S^x = 1$ gesetzt werden kann. Dann wird nach (3)

$$h_r(S) = \frac{g^m - 1}{g^x - 1} \sum_{\nu=0}^{x-1} g^\nu S^{-\nu}.$$

Hieraus folgt: Ist $\mathfrak{P}$ schon in $k(\varrho_1)$ nicht vom ersten Relativgrad, so hat x die Form eq^a, wo e ein echter Teiler von $q - 1$ bzw. $\frac{q-1}{2}$ ist, und $g^x - 1$ ist zu q teilerfremd. Andererseits ist $g^m - 1$ durch q^r teilbar, also auch $h_r(S)$. Demnach ist $z = 0$, $r \leqq v$ und Δ_r zu $\mathfrak{P}$ teilerfremd. Ist $z > 0$, so ist

$$x = q^{z-1}(q-1) \quad \text{bzw.} \quad \tfrac{1}{2} q^{z-1}(q-1)$$

Dann ist $g^x - 1$ genau durch q^z teilbar, also

$$h_r(S) \equiv 0 \pmod{q^{r-z}}$$

und

$$v \geqq r - z.$$

Danach ist $r - z$ der kleinste Wert, den v annehmen kann. Den genauen Wert von v ergibt folgender

Satz 5. Ist $\psi(g) = q^w l$, so ist

$$v = r - z + w$$

oder

$$v = r, \qquad \text{wenn } w \geqq z \text{ ist.}$$

Dabei sei wie vorher $r \geqq z$ vorausgesetzt.

Zum Beweise beachte man nur, daß nach (2)

$$\psi(S)\, h_r(S) \equiv \psi(g)\, h_r(S) \pmod{q^r}$$

ist.

Hieraus folgt, daß, von q^r-ten Potenzen abgesehen, ω stets so gewählt werden kann, daß die Zerlegung die Form

$$(\omega) = \mathfrak{a} \cdot \mathfrak{p}^{q^v h_z(S)}$$

hat, wo $\mathfrak{a}$ nur durch q^r-te symbolische Potenzen von $\mathfrak{p}$ und durch solche Ideale teilbar ist, die zu $\mathfrak{P}$ prim sind. Außerdem ist $v = r - z + w$ bzw. $v = r$.

Ist $r < z$, so kann man der Zerlegung der Zahl ω die gleiche Form geben. Es bezeichne $\overline{\mathfrak{p}}$ einen Teiler von $\mathfrak{P}$ in $k(\varrho_r)$. Dann ist $\overline{\mathfrak{p}}$ die Relativnorm von $\mathfrak{p}$ in bezug auf $k(\varrho_r)$, wo $\mathfrak{p}$ ein Primteiler von $\mathfrak{P}$ in $k(\varrho_z)$ ist. S bezeichnet wie immer die Substitution ϱ durch ϱ^g; gleichgültig, ob es sich dabei um ϱ_z oder ϱ_r handelt. Es kommt darauf an, zu zeigen, daß die $h_r(S)$-te Potenz von $\overline{\mathfrak{p}}$ durch die $h_z(S)$-te Potenz von $\mathfrak{p}$ ersetzt werden kann. Zu diesem Zweck schreiben wir $h_z(S)$ in der Form

$$h_z(S) = h_r(S) \sum_v (g S^{-1})^{v q^{r-1}(q-1)}, \qquad v = 0, 1, \ldots, q^{z-r} - 1.$$

Dann ist

$$h_z(S) \equiv h_r(S) \sum_v S^{-v q^{r-1}(q-1)} \pmod{q^r},$$

weil

$$g^{v q^{r-1}(q-1)} \equiv 1 \pmod{q^r} \quad \text{ist.}$$

Nach dieser Reduktion bedeutet diese Summe im Exponenten von $\mathfrak{p}$ die Relativnorm $\overline{\mathfrak{p}}$. Daher ist

$$\mathfrak{a}\, \mathfrak{p}^{h_z(S)} = \overline{\mathfrak{p}}^{h_r(S)},$$

wo $\mathfrak{a}$ eine symbolische q^r-te Potenz von $\mathfrak{p}$ ist. Beachtet man noch, daß $\varkappa$ durch $\overline{\mathfrak{p}}^{\psi(S)}$ teilbar ist, so muß man die letzte Gleichung noch in die $\psi(S)$-te Potenz erheben und wie vorher $\psi(S)$ durch $\psi(g) = q^w l$ ersetzen, so erhält man für ω wieder die Zerlegung:

$$(\omega) = \mathfrak{a}' \mathfrak{p}^{q^w h_z(S)},$$

und es ist in diesem Falle $v = w$.

Definition: Ein Körper P_r soll ein Primkörper heißen, wenn er folgende Bedingungen erfüllt:

1. Er ist relativ zyklisch über k vom Grade q^r.

2. Seine Relativdiskriminante ist eine Potenz von nur einem zu q teilerfremden Primideal $\mathfrak{P}$.

3. Ist P_v der größte in P_r enthaltene unverzweigte Teiler, so soll $v = r - z$ (d. h. $w = 0$) sein.

In einem Ausnahmefall müssen wir die Forderung 2, daß die Diskriminante die Potenz von nur einem Primideal ist, fallen lassen. Denn für $q = 3$ und $D = 3$ existiert unter Umständen gar kein Primkörper der oben definierten Art. Für diesen besonderen Fall muß die Forderung 2 dahin abgeändert werden, daß Δ_r außer durch $\mathfrak{P}$ auch noch durch $1 - \varrho_r$ teilbar sein kann. Für den Beweis des folgenden Satzes ist es nicht notwendig diese Unterscheidung zu beachten. Wir werden an späterer Stelle auf diese Tatsache zurückkommen.

Daß zu jedem $\mathfrak{P}$, q und $z > 0$ immer ein Primkörper vorhanden ist, kann man mit Hilfe der Ordnungs- und Kreisteilungskörper zeigen.

Zu der obigen Definition kann man noch hinzufügen, daß v möglichst klein sein soll, es ist aber nicht notwendig.

Satz 6. Die Gesamtheit aller Abelschen Körper wird eingefangen durch Primkörper der oben definierten Art und durch solche Körper, deren Diskriminante entweder

eine Einheit ist, oder nur solche Primideale enthält, die in q aufgehen. Dabei ist noch zu beachten, daß zu jedem vorgegebenen $\mathfrak{P}$ und q immer nur ein Primkörper vorhanden zu sein braucht, um die Gesamtheit darzustellen. Insbesondere ergibt sich aus diesem Satz, daß sich zwei Primkörper, die zu demselben $\mathfrak{P}$ und q gehören, nur durch Einheitskörper unterscheiden; d. h. der eine dieser beiden Körper ist in einem Produkt enthalten, das aus dem anderen und einem Einheitskörper gebildet ist.

Beweis: Es sei $\Gamma'_{r'}$ ein beliebiger zyklischer Körper von Grade $q^{r'}$, $\mathfrak{P}$ ein zu q primer Teiler seiner Diskrimiante. $\Gamma'_{r'}$ werde durch

$$\omega' = \varkappa'^{h_{r'}(S)}$$

bestimmt, und es sei

$$(\omega') = \mathfrak{a}' \, \mathfrak{p}^{q^{v'} h_z(S)}.$$

Dann ist:

$$\begin{aligned} v' &= r' - z + w', && \text{wenn } r' \geqq z \text{ und } w \leqq z, \\ v' &= r', && \text{wenn } w \geqq z, \\ v' &= w', && \text{wenn } r' < z. \end{aligned}$$

Der Fall $v' = r'$ kann außer Betracht bleiben, weil dann $\Delta'_{r'}$, die Diskriminante von $\Gamma'_{r'}$, zu $\mathfrak{P}$ prim ist.

Für den Primkörper P_r seien die entsprechenden Bezeichnungen:

$$\omega = \varkappa^{h_r(S)}, \qquad (\omega) = \mathfrak{a} \, \mathfrak{p}^{q^v h_z(S)}, \qquad v = r - z.$$

Die beiden Körper können auch einen gemeinsamen Teiler haben. Wir haben nun einen Körper $\Gamma''_{r''}$ zu konstruieren, so daß

$$P_r \, \Gamma'_{r'} = P_r \, \Gamma''_{r''}$$

ist, und $\Gamma''_{r''}$ eine zu $\mathfrak{P}$ prime Diskriminante hat. Statt P_r kann auch ein Teiler dieses Körpers genommen werden. Wir brauchen zur Darstellung nur den Teiler $P_{v-v'+r'}$, der durch die Zahl

$$\xi = \omega^{q^{-v+v'-r'}}$$

erzeugt wird. Es ist leicht einzusehen, daß die Zahl $v - v' + r'$ auf jeden Fall positiv ist. Wir setzen noch

$$\xi' = \omega'^{q^{-r'}}.$$

Die Zahl $\eta = \xi \, \xi'^{-1}$ erzeugt gemäß der vorher getroffenen Festsetzung einen zyklischen Teiler $\Gamma''_{r''}$ des Produktes $\Gamma'_{r'} \, P_{v-v'+r'}$, und es ist

$$\Gamma''_{r''} \, P_{v-v'+r'} = \Gamma'_{r'} \, P_{v-v'+r'},$$

weil sich die Zahlen η und ξ durch ξ' und ξ rational ausdrücken lassen und umgekehrt. Ferner ist

$$\eta = \omega^{q^{-v+v'-r'}} \cdot \omega'^{-q^{-r'}}$$

Der symbolische Exponent, mit dem das Primideal $\mathfrak{p}$ in η auftritt, ist:

$$q^{-v+v'-r'} \, q^v h_z(S) - q^{v'} \, q^{-r'} h_z(S) = 0,$$

wobei es vorübergehend gestattet sein mag, $\mathfrak{p}$ mit gebrochenen Zahlen zu potenzieren.

Daher läßt sich η so darstellen, daß die unter den Wurzeln stehenden Zahlen zu $\mathfrak{p}$ teilerfremd sind, und die Diskriminante von $\Gamma''_{r''}$ ist nicht mehr durch $\mathfrak{P}$ teilbar. Sie enthält ein Primideal weniger als die Diskriminante von $\Gamma'_{r'}$. Der Beweis ist somit durch Induktion erbracht.

Anstatt die Körper zu betrachten, hätte man auch den vorigen Satz so formulieren können, daß sich folgende Zerlegung der Zahl ω ergibt:

$$\omega = \sigma^n \, \omega_p^{\alpha} \, \omega_{p'}^{'\alpha'} \cdots w .$$

Hierin bedeutet σ eine Zahl aus $k(\varrho)$; ω_p, ω_p', ... sind Zahlen, durch die Primkörper erzeugt werden, w endlich bestimmt einen Körper, der im zweiten Teil zu behandeln ist.

Alle Sätze behalten ihre Gültigkeit, wenn statt k der Körper der rationalen Zahlen zugrunde gelegt wird. Die Primkörper werden dann so erhalten: Es sei $p-1$ durch q^z aber nicht durch q^{z+1} teilbar, dann ist p im Körper der q^z-ten Einheitswurzeln in Primideale ersten Grades zerlegbar, aber nicht im Körper der q^{z+1}-ten Einheitswurzeln. Der Körper der p-ten Einheitswurzeln enthält einen zyklischen Teiler des Grades q^z, dessen Grundzahl eine Potenz von p ist, daher ist dieser Teiler der Primkörper P_z, und alle Primkörper sind Kreisteilungskörper.

Zweiter Teil.

Die Diskriminante von Γ_r enthält nur solche Primideale, die auch in q aufgehen.

Bei der Darstellung des allgemeinen zyklischen Körpers sind wir so weit gekommen, daß seine Diskriminante von allen Primidealen befreit ist, die nicht in q aufgehen. Wir wenden uns zu den noch übrig bleibenden Körpern und treffen folgende Festsetzung: Alle in diesem Teil vorkommenden Abelschen Körper sollen von der Beschaffenheit sein, daß ihre Diskriminante entweder eine Einheit ist, oder nur solche Primideale enthält, die auch in q aufgehen.

Die Tatsache, daß Γ_r durch ω nicht eindeutig bestimmt ist, sobald $r > 1$ ist, konnte im ersten Teil unbeachtet bleiben. Hier ist es aber wesentlich, daß von diesen Körpern der eine unverzweigt sein kann, die anderen nicht. Ist $r = 1$, so ist Γ_1 durch ω eindeutig festgelegt. Daher soll jetzt der allgemeine Körper Γ_r so aufgebaut werden, daß Γ_r als Körper q-ten Grades über Γ_{r-1} aufgefaßt wird. Aus diesem Grunde wird auch immer die Adjunktion der q-ten Einheitswurzel $\varrho = \varrho_1$ ausreichen. Es ist notwendig, für einige Sätze einen anderen Bereich B zugrunde zu legen, und zwar soll

$$B = E_v/k$$

sein, wo E_v ein zyklischer Einheitskörper q^v-ten Grades über k ist. Für $v = 0$ ist $B = k$.

Satz 7. Ist $E_v(\varrho)$ unverzweigt über $k(\varrho)$, so ist auch E_v unverzweigt über k und umgekehrt.

Der Beweis folgt leicht aus der Zerlegung eines in q enthaltenen Primideals aus $k(\varrho)$ in $E_v(\varrho)$, bzw. aus k in E_v.

Satz 8. $1 - \varrho$ kann in $B(\varrho)$ nicht durch das Quadrat eines Primideals teilbar sein.

Beweis: Nehmen wir zunächst $B = k$ an, so ist im Falle $k(\varrho) = R(\varrho)$, also $m = \frac{q-1}{2}$, bekanntlich $1 - \varrho$ selbst ein Primideal, also gewiß nicht durch das Quadrat eines Primideals teilbar. Ist $m = q - 1$, so gibt es einen in $k(\varrho)$ enthaltenen quadratischen Körper $k' = R(\sqrt{D'})$, so daß

$$k(\varrho) = k'(\varrho)$$

ist, und D' zu q teilerfremd ist. Denn $R(\varrho)$ enthält den quadratischen Körper $R(\sqrt{\pm q})$, wo das positive oder negative Vorzeichen zu nehmen ist, je nachdem q durch vier geteilt den Rest eins oder drei läßt. Ist D nicht durch q teilbar, so ist $k = k'$. Andernfalls ist

$$k' = R\left(\frac{\sqrt{-D}}{\sqrt{\pm q}}\right) = R(\sqrt{D'}).$$

Ist λ ein in q enthaltenes Primideal aus $k(\varrho)$ und wäre

$$1 - \varrho = \lambda^2$$

die Zerlegung von $1-\varrho$ in $k(\varrho)$, so wäre

$$(q) = \lambda^{2(q-1)}$$

die Zerlegung von q in $k(\varrho)$, daraus würde sich aber ergeben, daß q in k' das Quadrat eines Primideals ist; womit der Fall $B = k$ erledigt ist.

Ist v von Null verschieden, so brauchen wir nur zu beachten, daß λ infolge der Unverzweigtheit von $B/k(\varrho)$ nicht durch das Quadrat eines Primideals teilbar sein kann.

Demnach wollen wir die Zerlegung von q in den verschiedenen Körpern so bezeichnen:

Zerlegung in $R(\varrho)$: $(q) = (1-\varrho)^{q-1}$,
Zerlegung in $k(\varrho)$: $(1-\varrho) = \lambda\lambda'$ oder $1-\varrho = \lambda$,
Zerlegung in $B(\varrho)$: $\lambda = \Lambda\,\Lambda_1\,\Lambda_2 \cdots \quad \lambda' = \Lambda'\,\Lambda_1'\,\Lambda_2' \cdots$.

Im allgemeinen ist $\lambda = \lambda^S$, es kann aber auch eintreten, daß λ von λ^S verschieden ist, wie folgendes Beispiel zeigt:

$$q = 5, \quad D = 5, \quad k = R(\sqrt{-5}), \quad k(\varrho) = R(\varrho, i), \quad k' = R(i).$$

Der größte gemeinsame Teiler von $1-\varrho$ und $2+i$ ist λ, und λ^S ist der größte gemeinsame Teiler von $1-\varrho$ und $2-i$, weil $i^S = -i$ ist.

Satz 9. ω sei eine ganze Zahl aus $B(\varrho)$ und erzeuge einen Körper Γ_1/B. Wenn

$$\omega \equiv 1 \pmod{\Lambda^q},$$

so ist die Relativdiskriminante von $\Gamma_1(\varrho)$ über $B(\varrho)$ nicht durch Λ teilbar.

Beweis: (Vgl. Zahlbericht Satz 148.) Es gibt eine ganze Zahl ψ aus $B(\varrho)$, die durch $\Lambda_1\Lambda_2 \cdots \Lambda'\Lambda_1' \cdots$ teilbar ist, aber nicht durch Λ. Dann ist

$$y = \frac{\psi(1-\sqrt[q]{\omega})}{1-\varrho}$$

eine ganze Zahl, denn y genügt der Gleichung

$$\left(y - \frac{\psi}{1-\varrho}\right)^q + \frac{\psi^q\,\omega}{(1-\varrho)^q} = 0,$$

deren Koeffizienten ganze Zahlen sind. Die Diskriminante dieser Gleichung ist aber von einer Einheit abgesehen

$$(\psi^q\,\omega)^{q-1}$$

also nicht durch Λ teilbar.

Ist insbesondere

$$\omega \equiv 1 \pmod{(1-\varrho)^q},$$

so ist Γ_1/B unverzweigt, weil damit die betreffende Bedingung für die Primideale $\Lambda\,\Lambda_1 \cdots \Lambda'\,\Lambda_1' \cdots$ erfüllt ist.

ω erzeuge einen Körper Γ_1/B, also ist ω eine Zahl aus $B(\varrho)$. Es kann von zwei besonderen Fällen abgesehen, ω stets so gewählt werden, daß

$$\omega \equiv 1 \pmod{(1-\varrho)}$$

ist. Ist ω durch Λ teilbar und ist $\lambda = \lambda^S$, also auch $\Lambda = \Lambda^S$, so ersetzen wir ω durch ω^{1-S}. Ist $\lambda \neq \lambda^S$, dann ist $\lambda = \lambda^{S^2}$ und $\Lambda = \Lambda^{S^2}$, und ω wird durch ω^{1-S^2} ersetzt; dies ist nach Satz 1 erlaubt, solange $1-g$ bzw. $1-g^2$ nicht durch q teilbar ist. Beides kann nur eintreten für $q = 3$, und das erstere nur dann, wenn $k = R(\sqrt{-3})$ und $g = 1$ ist. Das zweite ist nur möglich, wenn $D = 3D'$ und die Zahl 3 in $k' = R(\sqrt{D'})$ in zwei

verschiedene Primideale zerfällt. Diese beiden Sonderfälle werden später unter VI und VII behandelt. Sehen wir einstweilen davon ab, so erhalten wir ein zu $1 - \varrho$ teilerfremdes ω.

Ist q' die absolute Norm von Λ, so ist

$$\omega^{q'-1} \equiv 1 \pmod{\Lambda},$$

und diese Kongruenz gilt auch modulo aller zu Λ konjugierten Ideale, also auch mod $(1 - \varrho)$. Nötigenfalls wird also ω durch $\omega^{q'-1}$ ersetzt.

Wir haben seither nicht davon Gebrauch gemacht, daß Γ_{v+1} ein zyklischer Körper q^{v+1}-ten Grades über k sein soll. Aus dieser Tatsache ergibt sich noch eine wichtige Bedingung für die Zahl ω, die wir jetzt ableiten wollen. Wir bezeichnen den Körper wieder mit Γ_{v+1}/k, danach ist $\Gamma_v = B$. Die Substitutionen der Gruppe von Γ_{v+1} seien:

$$1, s, s^2, \ldots, s^{q^{v+1}-1}$$

Satz 10. ω^{1-s} ist die q-te Potenz einer Zahl α aus $B(\varrho)$.

Beweis: Betrachtet man $\Gamma_{v+1}(\varrho)$ als Körper q^{v+1}-ten Grades über $k(\varrho)$, so stellen die q^{v+1} Zahlen

$$\varrho^{\nu} \sqrt[q]{\omega^{s^\mu}}, \qquad \begin{matrix} \mu = 0, 1, \ldots, q^v - 1, \\ \nu = 0, 1, \ldots, q - 1, \end{matrix}$$

ein System konjugierter Zahlen dar, und diese sind alle untereinander verschieden, denn andernfalls wäre ω eine Zahl eines in $\Gamma_v(\varrho)$ enthaltenen Teilers $\Gamma_{v'}(\varrho)$ $(v' < v)$, und dann könnte der durch $\sqrt[q]{\omega}$ erzeugte Körper nicht vom Grade q^{v+1} sein.

Außerdem lassen sich alle durch eine ausdrücken, oder die beiden Körper

$$B(\varrho, \sqrt[q]{\omega}) \text{ und } B(\varrho, \sqrt[q]{\omega^s})$$

sind einander gleich. Es gibt also eine ganze Zahl c und eine Zahl α aus $B(\varrho)$, so daß

$$\omega^c = \omega^s \alpha^q \text{ und } 1 \leqq c < q$$

ist. Potenziert man diese Gleichung wiederholt mit s, und beachtet man, daß ω und α durch s^{q^v} unverändert bleiben, so folgt leicht:

$$c^{q^v} \equiv 1 \pmod{q};$$

daher muß $c = 1$ sein, also

$$\omega^{1-s} = \alpha^q.$$

Betrachten wir diese Gleichung noch mod Λ, so folgt aus

$$\alpha \equiv 1 \pmod{\Lambda}$$
$$\alpha^q \equiv 1 \pmod{\Lambda^q}$$

und aus

$$\alpha \equiv 1 \pmod{(1 - \varrho)}$$
$$\alpha^q \equiv 1 \mod (1 - \varrho)^q.$$

Daher ist

$$\omega \equiv \omega^s \pmod{(1 - \varrho)^q}. \tag{5}$$

Da auch $\omega^{s^\nu - s^\nu}$ eine q-te Potenz ist, so fügen wir noch hinzu:

$$\omega^{s^\nu} \equiv \omega^{s^\nu} \pmod{(1 - \varrho)^q} \qquad \nu = 0, 1, \ldots, m - 1. \tag{6}$$

Satz 11. Ist

$$\omega \equiv 1 \pmod{\Lambda^\nu} \text{ und } \nu \leqq q,$$

so gilt diese Kongruenz auch mod λ^ν. Wie erwähnt, ist Λ ein Primideal in $B(\varrho)$, und λ ist durch Λ teilbar.

Beweis: Mit Rücksicht auf (5) ist

$$\omega^{s^{-1}} \equiv \omega \pmod{(1-\varrho)^q}, \text{ also auch } \pmod{\Lambda^\nu},$$

oder

$$\omega^{s^{-1}} \equiv 1 \pmod{\Lambda^\nu} \text{ und } \omega \equiv 1 \pmod{\Lambda^{\nu s}},$$

d. h. $\omega - 1$ ist auch durch die ν-te Potenz aller zu Λ konjugierten Primideale des Körpers $B(\varrho)/k(\varrho)$ teilbar, woraus sich unter Anwendung des Satzes 8 ergibt:

$$\omega \equiv 1 \pmod{\lambda^\nu}.$$

Satz 12. Ist $\omega - 1$ genau durch λ^ν teilbar und $\nu < q$, so ist die Zahl

$$A = \frac{\omega - 1}{(1-\varrho)^\nu}$$

mod λ einer Zahl aus $k(\varrho)$ kongruent.

Beweis: A kann so dargestellt werden, daß Zähler und Nenner zu λ teilerfremd sind, und in der Kongruenz

$$\omega \equiv 1 + A\,(1-\varrho)^\nu \pmod{\lambda^{\nu+1}}$$

kann A mod λ ersetzt werden. Wir wenden die Substitution s an, und beachten $\lambda = \lambda^s$, dann folgt aus (5)

$$A \equiv A^s \pmod{\lambda}.$$

Wir zeigen, daß an Stelle von A eine Zahl a treten kann, so daß

$$A \equiv a \pmod{\lambda}$$

ist, und benügen uns damit zu beweisen, daß a eine Zahl des Körpers $\Gamma_{\nu-1}(\varrho)$ ist. Daraus folgt dann durch Induktion, daß a einer Zahl aus $k(\varrho)$ mod λ kongruent ist.

$\mathfrak{N}_R(A)$ sei die Relativnorm von A in bezug auf $\Gamma_{\nu-1}(\varrho)$, dann ist

$$\mathfrak{N}_R(A) \equiv A^q \pmod{\lambda};$$

ferner sei q' die totale Norm von Λ, dann besagt der Fermatsche Satz

$$A^{q'} \equiv A \pmod{\Lambda},$$

und diese Kongruenz besteht auch mod Λ', mod Λ'', . . ., daher auch mod λ. Also ist

$$[\mathfrak{N}_R(A)]^{q'-1} \equiv A^{q'} \equiv A \pmod{\lambda},$$

wodurch gezeigt ist, daß A mod λ einer Zahl aus $\Gamma_{\nu-1}(\varrho)$ kongruent ist. So fortfahrend kommen wir schließlich zu einer Zahl a aus $k(\varrho)$, so daß

$$A \equiv a \pmod{\lambda}$$

wird.

Ist λ ein Primideal ersten Grades in $k(\varrho)$, so bilden $0, 1, \ldots, q-1$ ein vollständiges Restsystem mod λ, und a ist rational. Ist q^2 die absolute Norm von λ, so sind die Zahlen

$$x + y\sqrt{D'}, \qquad x, y = 0, 1, \ldots, q-1,$$

ein vollständiges Restsystem mod λ, und a ist eine Zahl aus k'. Um weitere Eigenschaften der Zahl a abzuleiten, benutzen wir die Beziehung (6) und betrachten zunächst $\nu < q$. Für den Fall $\lambda = \lambda^S$ folgern wir der Reihe nach aus

$$\begin{aligned}
\omega &\equiv 1 + a\,(1-\varrho)^\nu \bmod \lambda^{\nu+1},\\
\omega^S &\equiv 1 + a^S\,(1-\varrho^g)^\nu \bmod \lambda^{\nu+1},\\
\omega^g &\equiv 1 + ag\,(1-\varrho)^\nu \bmod \lambda^{\nu+1},\\
\omega^g &\equiv \omega^S \bmod \lambda^q, \text{ also auch mod } \lambda^{\nu+1},
\end{aligned}$$

$$ag(1-\varrho)^\nu \equiv a^S (1-\varrho^g)^\nu \bmod \lambda^{\nu+1},$$
$$ag \equiv a^S (1+\varrho+\cdots+\varrho^{g-1})^\nu \bmod \lambda,$$
$$ag \equiv a^S g^\nu \bmod \lambda.$$

Im Falle $\lambda \neq \lambda^S$ beachte man, daß immer $\lambda = \lambda^{S^2}$ ist, und wir erhalten aus

$$\omega^{g^2-S^2} \equiv 1 \pmod{\lambda^{\nu+1}}$$
$$ag^2 \equiv a^{S^2} g^{2\nu} \pmod{\lambda},$$

eine Beziehung, die auch im Falle $\lambda = \lambda^S$ ihre Gültigkeit behält. Da immer $a = a^{S^2}$ ist, so folgt:

$$\text{entweder } g^{2\nu-1} \equiv 1 \pmod q \text{ oder } a \equiv 0 \pmod{\lambda}.$$

Denken wir uns also $\nu < q$ aber so groß, daß a nicht durch λ teilbar ist, so kann nur $\nu = 1$ oder $\nu = \frac{q+1}{2}$ sein. Ist dies nicht möglich, so ist $\omega - 1$ durch λ^q teilbar. Wir fassen die bis dahin abgeleiteten Eigenschaften der Zahl ω zusammen:

Satz 13. Ist $\omega - 1$ genau durch λ^ν teilbar und setzt man

$$\omega \equiv 1 + a(1-\varrho)^\nu \pmod{\lambda^{\nu+1}},$$

so ist für $\nu < q$ die Zahl a rational oder von der Form $x + y\sqrt{D'}$. Wenn außerdem $\lambda = \lambda^S$ ist, so wird noch

$$a \equiv a^S g^{\nu-1} \bmod \lambda.$$

Im allgemeinen kommen für ν nur die Werte 1, $\frac{q+1}{2}$ oder $\nu \geqq q$ in Betracht. Wichtig ist, daß die Zahl a für $\nu < q$ von dem Körper B unabhängig ist. Hat man mehrere Zahlen $\omega, \omega', \omega'', \ldots$, die alle die gleichen Voraussetzungen erfüllen, aber verschiedenen Bereichen $B, B', \ldots$ angehören, so gilt dieser Satz 13 auch für jedes $\omega^a \cdot \omega^{a'} \cdot \omega^{a''} \cdots$.

Definition: Zwei oder mehrere Zahlen $\omega, \omega', \omega'', \ldots$, die bzw. den unverzweigten Körpern $\Gamma_v(\varrho), \Gamma'_{v'}(\varrho), \ldots$ angehören, und so beschaffen sind, daß sie zyklische Körper $\Gamma_{v+1}, \Gamma'_{v'+1}, \ldots$ über k bestimmen, sollen voneinander abhängig heißen, wenn es ganze Zahlen $c, c', c'', \ldots$ gibt, die nicht sämtlich durch q teilbar sind, so daß

$$\omega^c \omega'^{c'} \omega''^{c''} \cdots \equiv 1 \pmod{(1-\varrho)^q}$$

ist. Die Zahlen c können mod q reduziert werden. Auch der Fall, daß die betreffenden Körper gemeinsame Teiler haben, sei zugelassen. Umgekehrt sind solche Zahlen voneinander unabhängig, wenn diese Kongruenz nur dann bestehen kann, wenn alle $c, c', c'', \ldots = 0$ sind.

Satz 14. Drei Zahlen $\omega, \omega', \omega''$ der oben definierten Art sind immer voneinander abhängig.

Beweis: Obwohl die Zahlen $\omega, \omega', \omega''$ verschiedenen Körpern angehören, führt die Betrachtung mod λ hier nur auf solche Reste, die rational sind oder in k' liegen. Die zu beweisende Kongruenz

$$\omega''' = \omega^c \omega'^{c'} \omega''^{c''} \equiv 1 \pmod{(1-\varrho)^q} \tag{7}$$

gilt gemäß der über die Zahlen ω getroffenen Festsetzungen mod λ. Bestimmen wir die Exponenten zunächst so, daß die Kongruenz (7) auch mod λ^2 besteht, so folgt daraus von selbst die Richtigkeit mod $\lambda^{\frac{q+1}{2}}$, unter Umständen sogar schon mod λ^q. Ist in $1-\varrho$ noch ein zweites Primideal λ' enthalten, so hat man zwei derartige Bedingungen

zu erfüllen. Die Bestimmung der Zahlen c, c', c'' wird im einzelnen durchgeführt. Dabei zeigt sich, daß in jedem Fall die Werte dieser Exponenten eindeutig sind, sofern nicht schon eine Abhängigkeit zwischen zweien der Zahlen $\omega, \omega', \omega''$ besteht.

Zur Durchführung des Beweises sind folgende Fälle zu unterscheiden:

I. $1 - \varrho = \lambda\lambda'$, d. h. λ ist vom ersten Grade, danach ist a rational und $m = q - 1$; ferner sei $\lambda = \lambda^S$. Wir setzen:

$$(8)\quad \begin{array}{l} \omega \equiv 1 + a\,(1-\varrho), \quad \omega' \equiv 1 + a'\,(1-\varrho), \quad \omega'' \equiv 1 + a''\,(1-\varrho) \pmod{\lambda^2}, \\ \omega \equiv 1 + b\,(1-\varrho), \quad \omega' \equiv 1 + b'\,(1-\varrho), \quad \omega'' \equiv 1 + b''\,(1-\varrho) \pmod{\lambda'^2}. \end{array}$$

Die Bedingung (7) führt, wenn man sie zunächst nur mod λ^2 und mod λ'^2 erfüllen will, zu:

$$(9)\quad \begin{array}{l} ac + a'c' + a''c'' \equiv 0 \pmod{q}, \\ bc + b'c' + b''c'' \equiv 0 \pmod{q}. \end{array}$$

Wir erhalten hieraus drei Werte c, c', c'', die nicht alle durch q teilbar sind, und es ist

$$\omega''' \equiv 1 + a'''\,(1-\varrho)^{\nu} \pmod{\lambda^{\nu+1}}$$

und $\nu \geqq 2$. Aus Satz 13 folgt, da a''' rational ist,

$$g^{\nu-1} \equiv 1 \pmod{\lambda}$$

und $\nu \geqq q$, dasselbe gilt für λ', also ist

$$\omega''' \equiv 1 \pmod{1-\varrho)^q}.$$

II. $1 - \varrho = \lambda^{1+S}$, d. h. $\lambda \neq \lambda^S$. Dann ist ebenfalls a rational, $m = q - 1$. Auch $q = 3$ ist zugelassen. (Vergl. VI.) Wir betrachten wie vorher die Kongruenz mod λ^2, und erhalten aus (8) drei Zahlen a, a', a'' und die Bedingung:

$$ac + a'c' + a''c'' \equiv 0 \pmod{q}.$$

Wir nehmen zwei voneinander unabhängige, von Null verschiedene Lösungen c_1, c_1', c_1'' und c_2, c_2', c_2'', d. h. die c_2 dürfen nicht ganzzahlige Vielfache der c_1 sein, und bilden

$$\omega_1 = \omega^{c_1}\,\omega'^{c_1'}\,\omega''^{c_1''}, \qquad \omega_2 = \omega^{c_2}\,\omega'^{c_2'}\,\omega''^{c_2''},$$

dann ist

$$\omega_1 \equiv \omega_2 \equiv 1 \pmod{\lambda^2}, \text{ also auch } \pmod{\lambda^{\frac{q+1}{2}}}.$$

Danach gibt es zwei rationale Zahlen b_1 und b_2, so daß

$$\omega_1 \equiv 1 + b_1\,(1-\varrho)^{\frac{q+1}{2}} \text{ und } \omega_2 \equiv 1 + b_2\,(1-\varrho)^{\frac{q+1}{2}} \pmod{\lambda^{\frac{q+1}{2}+1}},$$

dann ist

$$\omega''' = \omega_1^{b_2}\,\omega_2^{-b_1} \equiv 1 \pmod{\lambda^{\frac{q+1}{2}+1}}, \text{ also auch } \pmod{\lambda^q}.$$

Sind b_1 und $b_2 = 0$, so ist

$$\omega_1 \equiv \omega_2 \equiv 1 \pmod{\lambda^q},$$

und unter den drei Zahlen $\omega, \omega', \omega''$ sind bereits zwei voneinander abhängig. Andernfalls erkennt man leicht, daß

$$c = c_1 b_2 - c_2 b_1, \qquad c' = c_1' b_2 - c_2' b_1, \qquad c'' = c_1'' b_2 - c_2'' b_1$$

nicht alle durch q teilbar sein können.

Wir haben noch zu zeigen, daß auch

$$\omega''' \equiv 1 \pmod{\lambda^{Sq}} \text{ ist.}$$

Aus

$$\omega''' \equiv 1 \pmod{\lambda^q}$$

folgt:

$$\omega'''^g \equiv 1 \pmod{\lambda^q},$$
$$\omega'''^S \equiv 1 \pmod{\lambda^q}.$$

Potenziert man mit S^{-1}, so erhält man die gewünschte Kongruenz.

III. Es sei $1 - \varrho = \lambda$ und $m = \frac{q-1}{2}$ also $D = q$. $q = 3$ sei ausgeschlossen, weil in diesem Falle $\omega_1 = \omega_2 = \omega_3 = \varrho$ oder $= \varrho^2$ sein muß (vergl. VII). Dann ist g das Quadrat einer Primitivwurzel von q. λ ist vom ersten Grade und a ist rational. Aus Satz 13 ergibt sich wie im Falle (1):

$$g^{\nu-1} \equiv 1 \pmod{\lambda}$$

Danach ist $\nu = 1$ oder $\frac{q+1}{2}$ oder $\geqq q$. Im übrigen ist die Behandlung dieses Falles die gleiche wie bei II.

IV. $1 - \varrho$ sei vom zweiten Grade und $D' = D$, also nicht durch q teilbar. Dann ist $m = q - 1$ und $a = a^S$. Daher ist nach Satz 13

$$g^{\nu-1} \equiv 1 \pmod{\lambda}.$$

Also kann nur $\nu = 1$ oder $\nu \geqq q$ sein. D. h. aus $\omega''' \equiv 1 \pmod{\lambda^2}$ folgt dasselbe mod λ^q. Setzen wir wieder die Kongruenz (8) an, so haben a, a', a'' die Form:

$$a = \xi + \eta\sqrt{-D}, \quad a' = \xi' + \eta'\sqrt{-D}, \quad a'' = \xi'' + \eta''\sqrt{-D},$$

und wir erhalten für die Bestimmung der Zahlen c, c', c'' die Kongruenz:

$$ac + a'c' + a''c'' \equiv 0 \pmod{\lambda}$$

Trennt man hier den rationalen von dem irrationalen Bestandteil, so erhalten wir bei I zwei Kongruenzen mit rationalen Größen.

V. $1 - \varrho = \lambda$ sei vom zweiten Grade, aber $D = \pm qD'$. Dann ist a von der Form

$$a = \xi + \eta\sqrt{D'} \quad \text{und} \quad a^S = \xi - \eta\sqrt{D'},$$

aus

$$a \equiv a^S g^{\nu-1} \pmod{\lambda}$$
$$\xi + \eta\sqrt{D'} \equiv (\xi - \eta\sqrt{D'})\, g^{\nu-1} \pmod{\lambda}$$

folgt:

$$\left.\begin{aligned} \xi &\equiv \xi g^{\nu-1} \\ \eta &\equiv -\eta g^{\nu-1} \end{aligned}\right\} \pmod{q}.$$

Das ist aber nur möglich, wenn entweder $\xi = 0$ und $\nu = \frac{q+1}{2}$ oder $\eta = 0$ und $\nu = 1$ oder $\nu \geqq q$ ist.

Suchen wir zuerst die betreffende Kongruenz mod λ^2 zu erfüllen, so sind die Größen $\eta = 0$ und die Zahlen a, a', a'' rational. Daher liegt der Fall ebenso wie bei II. Wir bilden genau wie dort zwei unabhängige Zahlen ω_1 und ω_2, so daß

$$\omega_1 \equiv \omega_2 \equiv 1 \pmod{\lambda^{\frac{q+1}{2}}}.$$

Beim nächsten Schritt ist zu beachten, daß der rationale Bestandteil des betreffenden Restes verschwindet.

Damit ist Satz 14 bewiesen, und es bleibt noch übrig, entsprechende Betrachtungen auch für den Fall durchzuführen, der bisher ausgeschlossen war, nämlich daß ω mit q

einen gemeinsamen Teiler besitzt. Wie erwähnt, kann dies nur unter besonderen Umständen für $q = 3$ eintreten. Bevor wir diesen Sonderfall erledigen, kommen wir zu dem eigentlichen Ergebnis dieses Abschnittes, nämlich zur Darstellung derjenigen zyklischen Körper, deren Diskriminante von allen zu q primen Idealen frei ist. Der folgende Satz soll zeigen, daß man hier zwei Primkörper braucht, um alle einzufangen. Die Existenz dieser beiden Körper wird wieder durch Kreisteilungskörper und Ordnungskörper gewährleistet. Für den einen nehme man den Teiler q^r-ten Grades des Körpers der q^{r+1}-ten Einheitswurzeln, und der andere ist in dem Ordnungskörper enthalten, der durch den Führer q^{r+1} bestimmt wird.

Satz 15. Ist Γ_r ein zyklischer Körper q^r-ten Grades über k, in dessen Diskriminante nur Primteiler von q aufgehen, so ist Γ_r Teiler eines Produktes

$$Q_r^{(1)} Q_r^{(2)} E_{r'}, \quad r' \leqq r,$$

wo $E_{r'}$ ein Einheitskörper ist, und $Q_r^{(1)}$ und $Q_r^{(2)}$ Primkörper bezeichnen, die folgendermaßen definiert sind:

1. Sie sind zyklisch vom Grade q^r über k und haben keinen gemeinsamen Teiler.
2. Ihre Diskriminanten sind nur durch solche Primideale teilbar, die auch in q aufgehen.
3. Der Teiler $Q_v^{(1)}$ ist unverzweigt, während dies für $Q_{v+1}^{(1)}$ nicht der Fall ist.
4. $Q_1^{(2)}$, der Teiler q-ten Grades von $Q_r^{(2)}$, habe eine von der Einheit verschiedene Diskriminante.
5. Sind ω_1 und ω_2 diejenigen Zahlen aus $Q_v^{(1)}(\varrho)$ und $k(\varrho)$, durch die die Körper $Q_{v+1}^{(1)}$ und $Q_1^{(2)}$ bestimmt werden, so müssen ω_1 und ω_2 voneinander unabhängig sein.
6. Die Zahl v soll möglichst klein sein.

Die Zahl r ist dabei keinen Beschränkungen unterworfen. Diese Primkörper sind durch die Definition nicht eindeutig bestimmt. Abgesehen davon, daß man wie im ersten Teil noch Einheitskörper hinzunehmen kann, bleibt hier noch insofern eine Mehrdeutigkeit, als man aus dem Produkt

$$Q = Q_r^{(1)} Q_r^{(2)}$$

zwei andere zyklische Körper statt $Q_r^{(1)}$ und $Q_r^{(2)}$ auswählen kann, deren Produkt Q ist. Es kann übrigens immer statt $Q_r^{(2)}$ der Kreisteilungskörper genommen werden.

Beweis: Wir stellen zunächst fest, ob Γ_r mit dem Produkt

$$Q = Q_r^{(1)} Q_r^{(2)}$$

einen gemeinsamen Teiler hat. Sollte dies der Fall sein, also Γ_1 ein Teiler von Q sein, so muß es in Q einen zyklischen Teiler q^r-ten Grades U_r geben, so daß $U_1 = \Gamma_1$ ist. Wir wenden Satz 2 an und bestimmen einen Körper $\Gamma'_{r'}$, so daß

$$\Gamma'_{r'} U_r = \Gamma_r U_r$$

und $r' < r$ ist. Diesen Körper $\Gamma'_{r'}$ legen wir nun den weiteren Betrachtungen zugrunde. Wir kehren wieder zur ursprünglichen Bezeichnung zurück und setzen Γ_r teilerfremd zu Q voraus. Danach lautet die Behauptung

$$\Gamma_r Q = E_r Q.$$

Es sei Γ_w der größte unverzweigte Teiler von Γ_r. Wir zeigen, daß es einen in $\Gamma_r Q$ enthaltenen, zu Q teilerfremden zyklischen Körper Γ'_r geben muß, so daß Γ'_{w+1}

unverzweigt ist. Ist ω_3 eine Zahl aus $\Gamma_w(\varrho)$, so daß durch $\sqrt[q]{\omega_3}$ der Körper Γ_{w+1} erzeugt wird, so genügen ω_1, ω_2, ω_3 den Voraussetzungen des Satzes 14, und es gibt ein

$$\omega' = \omega_1^{c_1}\,\omega_2^{c_2}\,\omega_3^{c_3} \equiv 1 \pmod{(1-\varrho)^q}, \qquad 0 \leqq c_1, c_2, c_3 < q.$$

Mit Rücksicht auf die Unabhängigkeit von ω_1 und ω_2 ist c_3 von Null verschieden. Ist $w < v$, so hat der größte in Γ_r enthaltene Einheitskörper einen kleineren Grad als $Q_v^{(1)}$. Gemäß der Forderung 6 darf es nicht möglich sein, $Q_r^{(1)}$ durch einen Körper mit einem kleineren v zu ersetzen. Demnach kann Γ_r zusammen mit $Q_r^{(2)}$ die Forderungen 1–5 nicht erfüllen, und es folgt, daß ω_2 und ω_3 voneinander abhängig sind, d. h. man kann $c_1 = 0$ setzen. Ist also $c_1 > 0$, so muß $w \geqq v$ sein.

Wir bilden das Produkt

$$\Theta = \Gamma_{w+1}\, Q_{v+1}^{(1)}\, Q_1^{(2)}.$$

Im Falle $c_1 = 0$ ist der mittlere Faktor wegzulassen. In Θ ebenso in $\Theta(\varrho)$ sind eine Reihe zyklischer Teiler q^{w+1}-ten Grades enthalten.

Von dem Körper

$$k(\sqrt[q]{\omega'})$$

kann man folgendes aussagen: Er ist ein Teiler von $\Theta(\varrho)$, er ist unverzweigt über $k(\varrho)$ (Satz 9), und er enthält mindestens einen zyklischen Teiler Γ'_{w+1} der oben verlangten Art. Letzteres erkennt man aus der Gleichheit der Produkte

$$k(\sqrt[q]{\omega'}) \cdot Q_{v+1}^{(1)} \cdot Q_1^{(2)} = \Theta(\varrho).$$

Die Gruppe dieses Abelschen Körpers enthält ein Basiselement der Ordnung q^{w+1} bzw. für $w = v$ zwei Basiselemente der Ordnungen q^{v+1}. Daraus folgt die Existenz eines Körpers Γ'_{w+1}. Damit ist erreicht, daß

$$\Gamma'_r\, Q = \Gamma_r\, Q$$

wird und der in Γ'_r enthaltene, unverzweigte Teiler größer ist als der in Γ_r enthaltene. So fortfahrend müssen wir schließlich zu einem Einheitskörper E_r kommen, so daß

$$E_r\, Q = \Gamma_r\, Q$$

ist.

Zwei besondere Fälle.

Wir haben noch den Fall zu erledigen, daß ω mit q einen gemeinsamen Teiler hat und nicht durch eine zu q prime Zahl ersetzt werden kann.

VI. Wie bei II sei $1 - \varrho = \lambda^{1+s}$, ferner sei $q = 3$, $g = 2$, $D = 3\,D'$ und 3 zerfalle in $k(\sqrt{D'})$ in zwei verschiedene Primideale. In diesem Falle ist außer den bereits definierten Körpern $Q_r^{(1)}$ und $Q_r^{(2)}$ noch ein dritter Körper $\overline{Q}_r$ erforderlich, um die Gesamtheit einzufangen.

$\overline{Q}_r$ sei so definiert:

1. Er ist zyklisch vom Grade 3^r.
2. In seiner Diskriminante gehen nur Teiler von 3 auf.
3. $\overline{Q}_{\overline{v}}$ sei der größte unverzweigte Teiler von $\overline{Q}_r$ $(0 \leqq v < r)$.
4. $\overline{Q}_{\overline{v}+1}$ sei, als Körper über $\overline{Q}_{\overline{v}}$ betrachtet, durch eine Zahl $\overline{\omega}$ aus $\overline{Q}_{\overline{v}}(\varrho)$ bestimmt, die mit 3 einen gemeinsamen Teiler hat, und $\overline{\omega}$ kann nicht durch eine zu 3 prime Zahl ersetzt werden.

5. $\bar{v}$ soll möglichst klein sein, d. h. es soll keinen zweiten Körper mit denselben Eigenschaften, aber mit einem kleineren $\bar{v}$ existieren.

Die allgemeine Klassenkörpertheorie bestätigt die Existenz solcher Körper für beliebige $r > \bar{v}$.

Dieser Körper muß auch teilerfremd zu $Q_r^{(1)}$ sein. Dann wären die unverzweigten Teiler ganz oder teilweise identisch, so könnte man durch Bildung des Produktes $\overline{Q}_r \cdot Q_r^{(1)}$ den Körper $\overline{Q}_r$ auf einen solchen mit kleinerem $\bar{v}$ zurückführen.

Ist wie vorher Λ ein Ideal aus $\overline{Q}_{\bar{v}}(\varrho)$ und ein Teiler von λ, und s die erzeugende Substitution der Gruppe des Körpers $\overline{Q}_{\bar{v}}/k$, so sei $\bar{\omega}$ genau teilbar durch $\Lambda^{\chi(s)}$.

Nach Satz 10 ist

$$\bar{\omega} = \alpha^q \, \bar{\omega}^s$$

oder

$$s\,\chi(s) \equiv \chi(s) \pmod{q}.$$

Setzt man

$$\chi(s) = a_0 + a_1 s + \cdots,$$

so ist

$$a_0 \equiv a_1 \equiv a_2 \equiv \cdots \pmod{q},$$

d. h. von q-ten Potenzen abgesehen, ist $\Lambda^{\chi(s)}$ die Relativnorm in bezug auf $k(\varrho)$. Dasselbe gilt für Λ^S, so daß in $\bar{\omega}$ nur λ und λ^S als Teiler anzusetzen sind. Ist $a + bS$ der symbolische Exponent, mit dem λ in $\bar{\omega}$ aufgeht, so muß $a + 2b$ zu 3 prim sein, denn andernfalls könnte man, wie aus Satz 1 folgt, $\bar{\omega}$ durch eine zu 3 prime Zahl ersetzen. Beachtet man ferner, daß $\bar{\omega}$ eine symbolische $h(S)$-te Potenz ist:

$$\bar{\omega} = \varkappa^{1+2S^{-1}} = \varkappa^{1+2S},$$

so ist $\bar{\omega}$ oder $\bar{\omega}^2$, von 3-ten Potenzen abgesehen, genau durch λ^{1+2S} teilbar.

Hieraus folgt: Hat man zwei Körper mit den Eigenschaften 1—4, so kann man die beiden den Körpern zugeordneten Zahlen $\bar{\omega}$ stets so wählen, daß ihr Quotient zu 3 prim wird.

Wir bilden das Produkt

$$\overline{Q}_r Q_r^{(1)} Q_r^{(2)} = Q,$$

wo $Q_r^{(1)}$ und $Q_r^{(2)}$ die in Satz 15 erklärte Bedeutung haben. An Stelle des dort betrachteten Produktes tritt jetzt ein Abelscher Körper Q des Grades 3^r, und wir beweisen in Ergänzung zu Satz 15:

Satz 15 a. Ist Γ_r ein beliebiger zyklischer Körper 3^r-ten Grades, in dessen Diskriminante nur Primteiler von 3 aufgehen, so ist Γ_r Teiler von

$$Q\,E_{r'}, \qquad r' < r,$$

wo $E_{r'}$ ein Einheitskörper ist.

Beweis: Wir können wie bei Satz 15 Γ_r teilerfremd zu Q annehmen, dann lautet die Behauptung:

$$\Gamma_r Q = E_r Q.$$

Die Zahl ω_3 ist ebenso erklärt wie dort, nur daß hier noch der Fall zu beachten ist, daß ω_3 durch λ teilbar sein kann. Ist dies nicht der Fall, so bilde man, wie dort

$$\omega' = \omega_1^{c_1} \omega_2^{c_2} \omega_3^{c_3} \equiv 1 \pmod{(1-\varrho)^3},$$

andernfalls läßt sich die Kongruenz

$$\omega' = \omega_1^{c_1}\,\omega_2^{c_2}\left(\frac{\omega_3}{\bar{\omega}}\right)^{c_3} \equiv 1 \pmod{(1-\varrho)^3}$$

erfüllen, da $\frac{\omega_3}{\bar{\omega}}$ zu 3 teilerfremd ist.

Auf jeden Fall kommen wir zu einem Körper Γ_r', so daß

$$\Gamma_r' Q = \Gamma_r Q$$

ist und Γ_{w+1}' ein Einheitskörper ist.

Wir geben zunächst einige Beispiele, bei denen v und $\bar{v} = 0$ sind und beschränken uns auf kubische Körper, d. h. $r = 1$.

D			$\bar{\omega}$	ω_1	ω_2
21	$\lambda^4 = 4 + \sqrt{7}$,	$\lambda^{4(1+S)} = 9$	$\lambda^{4(1+2S)} = 9(4 - \sqrt{7})$	$8 + 3\sqrt{7}$	ϱ
39	$\lambda^8 = 17 + 4\sqrt{13}$,	$\lambda^{8(1+S)} = 81$	$\lambda^{8(1+2S)} = 81(17 - 4\sqrt{13})$	$\frac{1}{2}(3 - \sqrt{13})$	ϱ
57	$\lambda^2 = 4 + \sqrt{19}$,	$\lambda^{2(1+S)} = -3$	$\lambda^{2(1+2S)} = -3(4 - \sqrt{19})$	$170 - 39\sqrt{19}$	ϱ

Die Zahlen ω_1 sind Einheiten und gewiß $(1 + 2S)$-te Potenzen. Andere Primideale als λ und λ^S kommen also in den Diskriminanten nicht vor. Unverzweigte Körper kann es auch nicht geben, weil die Klassenzahlen der hier betrachteten Körper $k = R(\sqrt{-D})$ nicht durch 3 teilbar sind. Daher werden durch $\sqrt[3]{\bar{\omega}}$, $\sqrt[3]{\omega_1}$, $\sqrt[3]{\omega_2}$ bzw. die Körper $\bar{Q}_1$, $Q_1^{(1)}$, $Q_1^{(2)}$ erhalten. Im Falle $D = 21$ ist

$$x = \sqrt[3]{9(4 - \sqrt{7})} + \sqrt[3]{9(4 + \sqrt{7})}$$

eine den Körper $\bar{Q}_1$ erzeugende Zahl, sie genügt der Gleichung

$$x^3 - 27x - 72 = 0\,.$$

An Stelle dieser Zahl $\bar{\omega}$ kann auch ein Produkt etwa $\varrho\bar{\omega}$ treten, dann wird

$$x = \sqrt[3]{9\varrho(4 - \sqrt{7})} + \sqrt[3]{9\varrho^2(4 + \sqrt{7})}\,,$$

$$x^3 - 27x - 36 + 9\sqrt{-21} = 0\,.$$

Der Körper $\bar{Q}_r$ ist natürlich nicht eindeutig, es kommt ja auch nur auf das Produkt Q an, das in diesem Falle eindeutig ist.

Ein anderes Beispiel, bei dem $v = 1$ und $\bar{v} = 1$ sind, verdanke ich einer brieflichen Mitteilung des Herrn Arnold Scholz (Freiburg i. Br.). Ich gebe hier seine Ausführungen wieder, die sich auf die Struktur der Restklassengruppe mod 3^2 beziehen.

Für $D = 3 \cdot 7 \cdot 937 = 19\,677$ hat die Gruppe der Idealklassen des Körpers $k = R(\sqrt{-D})$ zwei unabhängige Basisklassen der Ordnung 3, nämlich:

$$37^3 = N(176 + \sqrt{-19677}) = N(j_{37}^3) = N(\gamma),$$

$$19^6 = N(6259 + 20\sqrt{-19677}) = N(j_{19}^6) = N(\delta).$$

Weder j_{37} noch j_{19}^2 können Hauptideale sein, da 19 677 die kleinste Zahlnorm ist. Daher sind weder γ noch δ dritte Zahlpotenzen, wohl aber dritte Idealpotenzen. Außerdem ist weder γ noch δ noch $\gamma\delta$ noch $\gamma\delta^2 \equiv \pm 1 \pmod 9$, daher werden zwei unabhängige Zahlrestklassen mod 9 von zwei unabhängigen Idealkuben verschluckt, die bei Aufstellung der Klassengruppe mod 9 für einen kubischen Körper in die Hauptklasse fallen müssen, es kann also weder 3 noch 9 Führer eines kubischen Relativkörpers über k sein. Daher sind $Q_1^{(1)}$ und $\bar{Q}$ unverzweigt, während $Q_1^{(2)}$ den Führer $3^{\frac{3}{2}}$ hat.

VII. Der Fall $D = -3$ ist insofern einfach, weil $k = R(\sqrt{-3})$ ein einklassiger Körper ist, daher ist $B = k$. Soll die Diskriminante eines Körpers $k(\sqrt[3]{\omega})$ nur eine Potenz von $1 - \varrho$ sein, so muß ω entweder eine Einheit sein, oder nur den Faktor $1 - \varrho$ als Teiler enthalten. Demnach ist die allgemeinste Form:

$$\omega = \varrho^x (1 - \varrho)^y, \qquad x, y = 0, 1, 2.$$

Wir erhalten zwei Zahlen:

$$\omega' = \varrho \quad \text{und} \quad \omega'' = 1 - \varrho,$$

und jedes andere ω dieser Art ist durch diese beiden darstellbar. Diese beiden Körper erscheinen auch als Teiler von zyklischen Körpern 3^r-ten Grades, die wir noch angeben wollen. Der eine ist der Teiler 3^r-ten Grades des Körpers der 3^{r+1}-ten Einheitswurzeln, und der andere ist durch

$$\omega = (1 - \varrho_r)^{hr(S)}$$

bestimmt. Die Zahl r unterliegt dabei keiner Einschränkung.

Wir kommen nun auf die Bemerkung bei der Definition der Primkörper im ersten Teil zurück und betrachten das Beispiel $p = 5$; dann ist $z = 1$, und der Primkörper P_1 kann nur sein

$$k(\sqrt[3]{5}) \quad \text{oder} \quad k(\sqrt[3]{\varrho 5}) \quad \text{oder} \quad k(\sqrt[3]{\varrho^2 5}).$$

Alle diese Körper haben eine durch $1 - \varrho$ teilbare Diskriminante.

Ersetzen wir 5 durch 25, so ist

$$\left.\begin{aligned} 25 &\equiv 1 - 8(1 - \varrho)^2 \\ 25\varrho &= 1 - (1 - \varrho) - 8(1 - \varrho)^2 \\ 25\varrho^2 &\equiv 1 + (1 + \varrho)(1 - \varrho) - 8(1 - \varrho)^2 \end{aligned}\right\} \mod (1 - \varrho)^3,$$

da keine dieser Zahlen $\equiv 1 \pmod{(1 - \varrho)^3}$ ist, so sind die Diskriminanten aller dieser Körper durch $1 - \varrho$ teilbar, und es ist unmöglich, diesen Primkörper P_1 so zu gestalten, daß seine Diskriminante von $1 - \varrho$ frei ist. Andererseits wird dadurch die Anzahl derjenigen Körper, die zum allgemeinen Aufbau notwendig sind, nicht größer, als in den Fällen I–V.

Schließlich sei noch auf die Vereinfachung hingewiesen, die sich ergibt, wenn an Stelle von k der Bereich der rationalen Zahlen tritt. Unverzweigte Körper kann es dann keine geben, auch werden die beiden Primkörper $Q_r^{(1)}$ und $Q_r^{(2)}$ durch einen ersetzt, nämlich den Kreisteilungskörper. Daß ein Primkörper ausreicht, erkennt man leicht daran, daß $1 - \varrho$ ein Primideal ersten Grades ist, also die Reste rationale Zahlen sind. Ferner folgt aus $\omega \equiv 1 \pmod{\lambda^2}$ immer $\omega \equiv 1 \pmod{\lambda^q}$. Es gibt also nur einen zyklischen Körper q^r-ten Grades, dessen Grundzahl eine Potenz von q ist, und dieser Körper ist ein Kreisteilungskörper. In Verbindung mit dem ersten Teil haben wir so einen Beweis des Kroneckerschen Satzes: „Alle absolut Abelschen Körper sind Kreisteilungskörper“ für den Spezialfall ungeraden Grades.

Dritter Teil.

Satz 16. Jeder unverzweigte Abelsche Körper über k ist Teiler eines unverzweigten Körpers K, dessen Gruppe mit der Gruppe der Idealklassen von k (in absolutem Sinne) isomorph ist.

K ist der Klassenkörper zum Führer 1.

Wie erwähnt, wird dieser Satz nur mit der Einschränkung bewiesen, daß diese Gruppe zyklisch ist.

Beweis: Wir betrachten zunächst einen unverzweigten zyklischen Körper Γ vom Primzahlgrad q. $1, s, s^2, \ldots, s^{q-1}$ seien die Substitutionen seiner Gruppe. Wie Hilbert gezeigt hat (Zahlbericht Kap. XV.), gibt es eine Einheit ε in Γ, so daß

$$\varepsilon = \alpha^{1-s}$$

ist und α eine von einer Einheit verschiedene ganze Zahl aus Γ ist, ferner bestimmt α ein Ideal $\mathfrak{a}$ aus k, das zwar selber kein Hauptideal ist, aber dessen q-te Potenz der Hauptklasse in k angehört. Wird α durch eine andere Zahl ersetzt, so erhalten wir ein zu $\mathfrak{a}$ äquivalentes Ideal. Der Einheit ε ist also die durch $\mathfrak{a}$ repräsentierte Klasse $\mathfrak{A}$ zugeordnet, und den Einheiten $\varepsilon^2, \ldots, \varepsilon^{q-1}$ entsprechen die Klassen $\mathfrak{A}^2, \ldots, \mathfrak{A}^{q-1}$. Ist k ein einklassiger Körper, so können Einheitskörper über k nicht existieren. Daher kann man die Fälle $k = R(\sqrt{-3})$ und $k = R(\sqrt{-1})$ ausschließen, und nur solche Körper k betrachten, die außer ± 1 keine Einheit haben. Dann gibt es, wie aus den Hilbertschen Untersuchungen folgt, nur eine Einheit ε in Γ, die diese Eigenschaft hat, wenn man $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{q-1}$ als nicht wesentlich verschieden ansieht. Damit ist zu Γ eine und nur eine Untergruppe $1, \mathfrak{A}, \mathfrak{A}^2, \ldots, \mathfrak{A}^{q-1}$ der Idealklassengruppe aus k zugeordnet derart, daß alle Ideale dieser Untergruppe und nur diese in Γ zu Hauptidealen werden.

Wir zeigen folgendes: Wenn es außer Γ noch einen zweiten unverzweigten zyklischen Körper q-ten Grades Γ' über k gibt, so muß in k auch ein zweiter von $1, \mathfrak{A}, \mathfrak{A}^2, \ldots$ verschiedener Zyklus q-ten Ordnung existieren.

Wir bilden das Produkt $\Gamma\Gamma'$ und bezeichnen mit $1, s, s^2, \ldots, s^{q-1}$ die Substitutionen, die die Zahlen von Γ' ungeändert lassen, während $1, t, t^2, \ldots, t^{q-1}$ die Zahlen des Körpers Γ in sich selbst überführen. Wir betrachten jetzt den Körper Γ' als Relativkörper über Γ. Dann gibt es eine Einheit E in $\Gamma\Gamma'$, so daß

$$E = A^{1-t}.$$

ist, wo A eine Zahl aus $\Gamma\Gamma'$ ist und ein Ideal aus Γ darstellt, dessen q-te Potenz ein Hauptideal in Γ ist.

Es soll zunächst gezeigt werden, daß E und A so gewählt werden können, daß A ein Ideal aus k wird.

Da A^q der Hauptklasse in Γ angehört, so gilt dasselbe auch für $A^{(1-s)^q}$.

Daher gibt es eine Zahl λ $(0 \leqq \lambda < q)$, so daß $A^{(1-s)^\lambda}$ kein Hauptideal in Γ ist, während $A^{(1-s)^{\lambda+1}}$ ein solches ist.

Wir setzen

$$B = A^{(1-s)^\lambda} \text{ und } E_1 = E^{(1-s)^\lambda},$$

dann ist

$$E_1 = B^{1-t},$$

und B hat wieder die entsprechenden Eigenschaften wie A. Außerdem ist B^{1-s} ein Hauptideal in Γ. Daher ist

$$B^{1-s} = E_2\, c,$$

wo E_2 eine Einheit in $\Gamma\Gamma'$ und c eine Zahl aus Γ bezeichnet. Erheben wir die letzte Gleichung in die Potenz $1 + s + s^2 + \cdots + s^{q-1}$, so folgt:

$$E_2^{1+s+s^2+\cdots+s^{q-1}}\, c^{1+s+s^2+\cdots+s^{q-1}} = 1.$$

Aus $c = c^t$ folgt weiter, daß $E_2^{1+s+s^2+\cdots+s^{q-1}}$ eine Einheit aus k, also ± 1 ist.

Wir brauchen nur den Wert $+1$ zu berücksichtigen, denn wir hätten von vorneherein statt E_1 auch E_1^2 nehmen können. Aus

$$c^{1+s+s^2+\cdots+s^{q-1}} = 1$$

folgt, daß c in der Form

$$c = d^{s-1}$$

darstellbar ist, wo $d = d^t$ ist. So erhalten wir:

$$(Bd)^{1-s} = E_2 \text{ und } (Bd)^{1-t} = E_1.$$

Diese beiden Gleichungen besagen, daß Bd ein Ideal aus k darstellt, das in der Gleichung

$$E_1 = B^{1-t}$$

an die Stelle von B treten kann. Wir werden so zu einem Zyklus $1, \mathfrak{B}, \mathfrak{B}^2, \ldots, \mathfrak{B}^{q-1}$ von Idealklassen geführt, der von $1, \mathfrak{A}, \mathfrak{A}^2, \ldots, \mathfrak{A}^{q-1}$ verschieden sein muß, weil B in Γ kein Hauptideal sein konnte. Da die Gruppe der Idealklassen des Grundkörpers zyklisch ist, kann nur ein Zyklus q-ter Ordnung vorhanden sein, wodurch die Existenz eines zweiten Körpers Γ' ausgeschlossen wird.

Wir betrachten jetzt einen zyklischen Einheitskörper Γ_r vom Primzahlpotenzgrad $n = q^r$ und zeigen, daß die Existenz eines solchen Körpers Γ_r auch die Existenz eines Zyklus n-ter Ordnung von Idealklassen aus k erfordert.

Wir bezeichnen mit $E, E_1, \ldots, E', \ldots$ Einheiten aus Γ_r und mit $\varepsilon, \varepsilon_1, \ldots, \varepsilon', \ldots$ Einheiten aus Γ_{r-1}. Betrachten wir Γ_r als Körper q-ten Grades über Γ_{r-1}, so können wir die Hilbertschen Sätze über relative Grundeinheiten anwenden und daraus schließen, daß es gewiß Einheiten E gibt, so daß E nicht die Form εE_1^q besitzt. Es seien $1, s, s^2, \ldots, s^{n-1}$ die Substitutionen der Gruppe des Körpers Γ_r/k. Es gibt eine Einheit E, so daß E nicht die Form εE_1^{1-s} hat. Denn nehmen wir das Gegenteil an, so würde aus

$$E_1 = \varepsilon_1 E_2^{1-s}, \quad E_2 = \varepsilon_2 E_2^{1-s}, \ldots$$

folgen:

$$E = \varepsilon' E_n^{(1-s)^n} = \varepsilon' E'^q.$$

Wir gehen nun von einer Einheit E des Körpers Γ_r aus, die nicht die Form εE_1^{1-s} besitzt. Die Relativnorm von E ist eine Einheit aus k, daher muß

$$E^{1+s+\cdots+s^{n-1}} = \pm 1$$

sein. Wir brauchen wie vorher nur den Wert $+1$ zu berücksichtigen. Daher hat E die Form

$$E = \alpha^{1-s}.$$

α ist eine von einer Einheit verschiedene Zahl aus Γ_r und bestimmt ein Ideal $\mathfrak{a}$ aus k. $\mathfrak{a}$ ist im Körper Γ_{r-1} kein Hauptideal, denn andernfalls wäre

$$\alpha = E_1 \beta,$$

wo β eine Zahl aus Γ_{r-1} wäre, daraus würde sich für E die Form εE_1^{1-s} entgegen der Festsetzung für E ergeben.

$\mathfrak{a}$ hat also die Eigenschaft, daß es ein Ideal aus k und damit auch aus Γ_{r-1} ist, $\mathfrak{a}$ ist in Γ_{r-1} kein Hauptideal, aber in Γ_r. Daher gehört $\mathfrak{a}^q$ in Γ_{r-1} der Hauptklasse an, weil jedes Ideal eines Grundkörpers, das in einem zyklischen Oberkörper q-ten Grades zum Hauptideal wird, die Ordnung q haben muß.

Demnach lassen sich auch den Teilern $\Gamma_{r-1}, \Gamma_{r-2}, \ldots, \Gamma_1$ in gleicher Weise Ideale oder besser Zyklen von Idealklassen aus k zuordnen, so daß dem Körper Γ_ν ein durch das Ideal $\mathfrak{a}_\nu$ bestimmter Zyklus entspricht. $\mathfrak{a}_\nu$ ist also ein Ideal aus k, das in Γ_ν aber nicht $\Gamma_{\nu-1}$ zum Hauptideal wird, während $\mathfrak{a}_\nu^q$ in $\Gamma_{\nu-1}$ der Hauptklasse angehört ($\nu = 1, 2, \ldots, r$). Die Ordnungen der Ideale $\mathfrak{a}_\nu$ im Körper k sind Potenzen von q.

Enthält die Gruppe der Idealklassen in k einen Zyklus von der Ordnung q^w, so muß $w \geqq r$ sein.

Beweis: Von den durch die Ideale

$$\mathfrak{a}_1^{l_1}\,\mathfrak{a}_2^{l_2} \cdots \mathfrak{a}_r^{l_r} \qquad \begin{matrix} l_\nu = 0, 1, \ldots, q-1, \\ \nu = 1, 2, \ldots, r, \end{matrix}$$

bestimmten Klassen kann keine die Hauptklasse in k sein, es sei denn, daß alle l_ν verschwinden. Wäre etwa $l_r \neq 0$ und dieses Produkt ein Hauptideal, so wäre $\mathfrak{a}_r$ schon in Γ_{r-1} ein Hauptideal, wäre $l_r = 0$ aber $l_{r-1} \neq 0$, so schließen wir entsprechend usw. Wenn wir $l_1 = l_2 \cdots = l_r = 0$ ausschließen, erhalten wir $q^r - 1$ voneinander verschiedene Idealklassen in k, deren Ordnung eine Potenz von q ist.

Wir machen nun Gebrauch von der Einschränkung, daß die Gruppe der Idealklassen in k zyklisch ist; hat dieser Zyklus die Ordnung q^w, so gibt es, die Hauptklasse ausgeschlossen, $q^w - 1$ verschiedene Klassen in k, deren Ordnung eine Potenz von q ist. Daher ist

$$q^w - 1 \geqq q^r - 1 \quad \text{und} \quad w \geqq r.$$

Wenn es also einen unverzweigten zyklischen Körper Γ_r/k des Grades q^r gibt, so kann r nicht größer als w sein.

In der Tat gibt es immer einen Körper Γ_r, so daß $r = w$ ist. Dieser Körper existiert immer und ist der Teiler q^r-ten Grades des Klassenkörpers K.

Wir haben zu zeigen, daß jeder unverzweigte Körper $\Gamma'_{r'}$ ein Teiler von Γ_r ist. Zunächst muß $r' \leqq r$ sein, weil $r = w$ ist. Außerdem ist gezeigt, daß $\Gamma'_1 = \Gamma_1$ sein muß.

Daher gibt es nach Satz 2 einen Körper $\Gamma''_{r'-1}$, so daß

$$\Gamma_r\,\Gamma'_{r'} = \Gamma_r\,\Gamma''_{r'-1}\,.$$

Durch wiederholte Anwendung derselben Schlußweise ergibt sich schließlich:

$$\Gamma_r\,\Gamma'_{r'} = \Gamma_r\,.$$

Literaturangaben.

Über die Stellung der vorliegenden Arbeit zur Literatur ist folgendes zu sagen:

Weber hat zuerst den Kroneckerschen Vollständigkeitssatz über absolut Abelsche Körper bewiesen (Algebra Band II, 23. Abschnitt). Ähnlich wie in der vorliegenden Arbeit geht Weber bei diesem Beweis von einer Zerlegung der Zahl ω in Faktoren aus, deshalb steht wohl dieser Beweis meinen Untersuchungen näher, als die übrige Literatur. Weber hat den Gedankengang Kroneckers weitergeführt. Was in der Weberschen Arbeit das „Kummersche Theorem“ bedeutet (22. Abschnitt), ist in meiner Arbeit die Parameterdarstellung aller relativ zyklischen Körper durch

$$\omega = \varkappa^{h(S)}.$$

Bei Weber sind die Koeffizienten von $h(S)$ modulo q reduziert, und statt der Zahl $\varkappa$ tritt ein Ideal auf; daher mußte Weber nachweisen, daß gewisse Ideale zu Hauptidealen werden. Dieser Beweis ist noch recht umständlich. Er wurde noch einmal mit denselben Hilfsmitteln von Herrn F. Mertens geführt (Crelles Journal für Mathematik

131 (1906), Über zyklische Gleichungen). Hier findet sich auch die von mir benutzte Parameterdarstellung der Zahl ω. Vgl. S. 107, Zeile 7 von unten:

$$F(\alpha) = \xi^{\lambda}(\alpha)\, \Pi\, F(\alpha^{-s})^{s'}, \qquad ss' \equiv 1 \pmod{\lambda}.$$

Das ist in anderer Bezeichnung dasselbe, wie

$$\omega = \varkappa^{h(S)}.$$

Hieraus wird dann wie bei Weber geschlossen, daß $F(\alpha)$ die λ-te Potenz einer Kreisteilungszahl ist. Im übrigen ist der Gedankengang in dieser Abhandlung doch wesentlich von meiner Darstellung verschieden, und auch noch recht langwierig.

Erst durch die von Hilbert geschaffenen Grundlagen, die den tieferen Zusammenhang zwischen der arithmetischen Natur der Körper und ihrer Galoisschen Gruppe aufklärten, ging man davon ab, den von Kronecker, Weber und Mertens eingeschlagenen Weg weiter zu verfolgen. Es folgten Beweise des Kroneckerschen Satzes für absolut Abelsche Körper von Hilbert (Zahlbericht Kap. XXIII), Weber (Crelle Band 132), Steinbacher (Crelle Band 139) und Speiser (Crelle Band 149).

Bei diesen Arbeiten sind solche Zerlegungen der Zahl ω nicht benutzt, sondern die Beweise stützen sich auf die von Hilbert geschaffenen Begriffe der Zerlegungsgruppe, Trägheitsgruppe und Verzweigungsgruppe. Dabei ergeben sich letzten Endes dieselben Reduktionen des allgemeinen zyklischen Körpers, wie in der vorliegenden Arbeit. Vergleichen wir etwa meine Untersuchungen, erster Teil mit der Arbeit von Herrn Speiser, § 3, Nr. 5, so kommt es in beiden Arbeiten darauf an, die Anzahl der in der Diskriminante enthaltenen Primideale (hier Primzahlen) zu verringern; dies erreiche ich dadurch, daß ich aus zwei Zahlen ω_1 und ω_2 eine Zahl $\omega_1^{\alpha}\, \omega_2^{\beta}$ zusammensetze, die einen Körper der verlangten Eigenschaft bestimmt. Derselbe Körper wird bei Speiser als Trägheitskörper erhalten. Vgl. S. 178, Zeile 9 von unten: „Die Trägheitskörper von $\mathfrak{P}_1$ besitzt eine zu p prime Diskriminante usw." Eine entsprechende Gegenüberstellung des zweiten Teiles meiner Arbeit mit Nr. 6 der Speiserschen Abhandlung gelingt nicht, weil in dem Fall des imaginär-quadratischen Grundkörpers zwei Relativkörper $Q_r^{(1)}$ und $Q_r^{(2)}$ auftreten.

In der folgenden Literatur handelt es sich hauptsächlich um den nächsten Kroneckerschen Satz, den Fall der komplexen Multiplikation. Hier tritt als neue Schwierigkeit die Existenz der unverzweigten Körper hinzu. Takagi hat deshalb zuerst nur den Fall des einklassigen Grundkörpers $k(\sqrt{-1})$ behandelt. (Über die im Bereiche der rationalen komplexen Zahlen Abelschen Zahlkörper. The Journal of the College of Science, Imperial University of Tokyo **19** (1903), Art. 5). Hier wird in §§ 1–5 aus der Lenniskatengleichung die Existenz derjenigen Körper nachgewiesen, die ich als Primkörper bezeichnet habe, sie ergeben sich als Teiler gewisser durch Teilungsgleichungen erzeugter Körper. In § 6 sind die Eigenschaften dieser Körper zusammengestellt. Takagi hat an späterer Stelle hierfür den Ausdruck „Elementare Körper" gebraucht. Der folgende Teil dieser Arbeit enthält den Vollständigkeitsbeweis, deckt sich also in seinem Endergebnis für diesen speziellen Fall mit meinen Untersuchungen. Der Verfasser benutzt dabei, wie er selber in der Einleitung sagt, die „Hilbertsche Methode".

Die weitere Entwicklung des Problems leitet allmählich in die allgemeine Klassenkörpertheorie über.

Versuche, wie ich sie im dritten Teil der Arbeit gemacht habe, um für unverzweigte Körper den Vollständigkeitsbeweis nur unter Benutzung rein arithmetischer Hilfsmittel zu führen, finden sich nicht in der Literatur. Dagegen wurde diese Frage vollkommen durch Herrn Ph. Furtwängler gelöst: Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers (Mathematische Annalen **63** [1906].

Hier ist noch die Einteilung der Idealklassen im absoluten Sinne gemeint, ferner ist ebenso wie in der vorliegenden Arbeit, aber im Gegensatz zur späteren Theorie die Forderung der Unverzweigtheit eines relativ Abelschen Körpers allein zur vollständigen Definition des Klassenkörpers benutzt.

Bei den nachfolgenden Abhandlungen über das Klassenkörperproblem, von denen die Untersuchungen von Takagi, Fueter und Hasse in erster Linie zu nennen sind, läßt sich ein engerer Zusammenhang mit der vorliegenden Arbeit nicht erkennen, da hier wie bereits erwähnt, andere Mittel zur Anwendung kommen.

Aus der großen Arbeit von Takagi: Über eine Theorie des relativ Abelschen Zahlkörpers (Journal of the College of Science, Imperial University of Tokyo **41** (1920), Art. 9) ergibt sich ebenfalls eine Übersicht aller Abelschen Körper nach Grad und Relativdiskriminante geordnet, wenn auch diese Reduktion in der Arbeit selber in anderer Form zum Ausdruck kommt. So kann man aus Satz 28, Seite 90 „Alle relativ Abelschen Körper in bezug auf einen beliebigen algebraischen Körper werden durch die Klassenkörper nach den Idealmoduln in demselben erschöpft“ leicht das eigentliche Ergebnis meiner Untersuchung herleiten, wenn man im allgemeinen als Führer nur Potenzen von einem Primideal zuläßt, den Klassenkörper mit dem Führer 1, soweit das möglich ist, abtrennt und den übrigen Körper als Produkt von relativ zyklischen Körpern von Primzahlpotenzgrad darstellt. Der Beweis wird unter Benutzung des Begriffs der „Geschlechter“ geführt.

In analoger Weise wie bei Takagi ist dieses Ergebnis im zweiten Kapitel der Fueterschen Arbeit über: Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern (Math. Annalen Band **75** [1914]) dargestellt und mit ähnlichen Mitteln bewiesen.

In seiner Stellung zur übrigen Literatur läßt sich das Ergebnis der vorliegenden Arbeit dahin zusammenfassen, daß der ursprüngliche Gedankengang Kroneckers wieder aufgegriffen wird und dadurch unabhängig von der Klassenkörpertheorie arithmetische Grundlagen geschaffen werden, um die Vollständigkeitsbeweise zu führen. Fast scheint es, als ob die von mir benutzte, von Kronecker herrührende Parameterdarstellung für diese Probleme die gleichen Dienste leistet, wie die „Hilbertsche Methode“.

Von einer Anwendung meiner Untersuchung auf den Fall der komplexen Multiplikation möge einstweilen abgesehen werden. Gewiß ergibt sich aus meiner Darstellung leicht der Vollständigkeitsbeweis, wenn man Fueters Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen, als bekannt voraussetzt. Dort findet sich in Kapitel VII, Seite 262/263 ein Hauptsatz, von dem die Behauptungen 1—4, die sich hauptsächlich auf die Relativdiskriminante beziehen, ausreichen, im Zusammenhang mit meiner Untersuchung den Vollständigkeitsbeweis zu erbringen. Jedoch ist der Beweis dieses Hauptsatzes bei Fueter mit Mitteln geführt, die gerade in der vorliegenden Arbeit vermieden sind. Ich hoffe aber, in einer späteren Untersuchung diesen Satz über die Relativdiskriminante der Teilungssgleichungen und damit den Kroneckerschen Satz ebenfalls unabhängig von der übrigen Literatur beweisen zu können.

Eingegangen 9. September 1930.

Zyklische Minimalbasis zusammengesetzten Grades.

Von *Samson Breuer* in Karlsruhe i. B.

---

1. Unter einer rationalen zyklischen Minimalbasis n-ten Grades versteht man bekanntlich n algebraisch unabhängige rationale Funktionen von n Unbestimmten, welche sämtlich dem Invariantenkörper der zyklischen Permutationsgruppe der Unbestimmten angehören und diesen Körper erzeugen, und deren Koeffizienten ferner dem absoluten Rationalitätsbereich entnommen sind. Im folgenden beweisen wir den

Satz: *Kennt man rationale zyklische Minimalbasen für die teilerfremden Grade l und m, und enthält wenigstens eine von ihnen die Summe der Unbestimmten als Basisfunktion* [1]*, so kennt man auch eine rationale zyklische Minimalbasis für den Grad $n = l\,m$* [2].

Beweis: Im folgenden mögen die Indizes h, i, j, k, k' stets die nachbezeichneten Werte durchlaufen: $h, i = 0, 1, \ldots, l-1$; $j = 0, 1, \ldots, m-1$; $k = 1, 2, \ldots, l-1$; $k' = 1, 2, \ldots, m-1$. Die n Unbestimmten seien mit $x_{i|j}$ bezeichnet. Die zyklische Permutationsgruppe werde durch

$$S = \begin{pmatrix} x_{i|j} \\ x_{i+1|j+1} \end{pmatrix} \tag{1}$$

erzeugt, wobei die Indizes also stets auf den kleinsten nicht negativen Rest mod. l bezw. mod. m zu reduzieren sind. Hier wird offenbar schon von der Voraussetzung $(l, m) = 1$ Gebrauch gemacht. Weiter sei

$$y_i = \frac{1}{m}\,(x_{i|0} + x_{i|1} + \cdots + x_{i|m-1})\,, \tag{2}$$

$$\bar{x}_{i|j} = x_{i|j} - y_i\,, \tag{3}$$

$$z_{h|j} = y_0^h\,\bar{x}_{0|j} + y_1^h\,\bar{x}_{1|j} + \cdots + y_{l-1}^h\,\bar{x}_{l-1|j}\,, \tag{4}$$

$$\varphi_{k|j} = z_{k|0}\,z_{0|j} + z_{k|1}\,z_{0|j+1} + \cdots + z_{k|m-1}\,z_{0|j+m-1}\,, \tag{5}$$

wobei die zweiten Indizes der zweiten Faktoren auf der rechten Seite von (5) nötigenfalls mod. m zu reduzieren sind.

2. Die Größen y_i (2) werden durch S (1) in der Reihenfolge $(y_0, y_1, \ldots, y_{l-1})$ vertauscht. Sie genügen also einer rationalen zyklischen Gleichung l-ten Grades, und wir können nach Voraussetzung l zyklische Funktionen der y_i angeben, welche eine zyklische Minimalbasis für die y_i bilden und welche die Vertauschung S dulden.

---

[1]) Alle bis jetzt bekannten Minimalbasen erfüllen diese Bedingung oder können entsprechend umgeformt werden.

[2]) Für $l \equiv 1 \pmod 2$, $m = 2$ ist der Satz schon lange bekannt. Vgl. Breuer, Zyklische Gleichungen 6. Grades und Minimalbasis, Math. Ann. **86** (1921), S. 108—113; Furtwängler, Über Minimalbasen für Körper rationaler Funktionen, Sitzungsber. d. Akad. d. Wiss. in Wien, IIa, **134** (1925), S. 69—80, insbes. § 4; Breuer, Metazyklische Minimalbasis und komplexe Primzahlen, J. f. d. r. u. angew. Math. **156** (1926), S. 13—42, insbes. S. 20. — Die beiden letzteren Arbeiten werden im folgenden mit F. und B. zitiert; ihre Kenntnis wird nicht vorausgesetzt.

Die Größen $\bar{x}_{i|j}$ (3) werden durch S in der gleichen Weise wie die $x_{i|j}$ selbst vertauscht und erfüllen nach (2) und (3) die l Bedingungen

$$\bar{x}_{i|0} + \bar{x}_{i|1} + \cdots + \bar{x}_{i|m-1} = 0 .$$

Mithin erfüllen auch die Größen $z_{h|j}$(4) die l Bedingungen

$$z_{h|0} + z_{h|1} + \cdots z_{h|m-1} = 0 , \tag{6}$$

und sie werden durch S gruppenweise in der Reihenfolge $(z_{h|0}, z_{h|1}, \ldots, z_{h|m-1})$ vertauscht. Beides gilt insbesondere auch für die m Größen

$$z_{0|j} = \bar{x}_{0|j} + \bar{x}_{1|j} + \cdots + \bar{x}_{l-1|j} , \tag{7}$$

die also einer zyklischen Gleichung m-ten Grades genügen, in welcher der Koeffizient des zweithöchsten Gliedes verschwindet. Nach Voraussetzung können wir daher $m-1$ zyklische Funktionen der $z_{0|j}$ angeben, welche wegen

$$z_{0|0} + z_{0|1} + \cdots + z_{0|m-1} = 0 \tag{6'}$$

eine zyklische Minimalbasis für die $z_{0|j}$ bilden und welche die Vertauschung S dulden. Für späteren Gebrauch und zum besseren Verständnis merken wir noch an, daß wir nach (2, 3, 7) auch schreiben können

$$z_{0|j} = x_{0|j} + x_{1|j} + \cdots + x_{l-1|j} - \frac{1}{m} \sum_{ij} x_{i|j} . \tag{7'}$$

Die $(l-1)\,m$ Größen $\varphi_{k|j}$ (5) endlich dulden S, weil dieses, wie soeben bemerkt, nur die zweiten Indizes der $z_{h|j}$ zyklisch vertauscht. Sie erfüllen aber ferner die $l-1$ Bedingungen

$$\varphi_{k|0} + \varphi_{k|1} + \cdots + \varphi_{k|m-1} = 0 , \tag{8}$$

denn diese Summe wird nach (5) gleich dem Produkte $(z_{k|0} + z_{k|1} + \cdots + z_{k|m-1})$ $(z_{0|0} + z_{0|1} + \cdots + z_{0|m-1})$, dessen Faktoren nach (6) beide verschwinden. Mit den $(l-1)(m-1)$ Größen $\varphi_{k|k'}$ sind daher auch die $\varphi_{k|0}$, d. h. sämtliche $(l-1)\,m$ Größen $\varphi_{k|j}$ rational bekannt.

3. Die im vorstehenden erwähnten l Basisfunktionen der y_i, die $m-1$ Basisfunktionen der $z_{0|j}$ und die $(l-1)(m-1)$ Funktionen $\varphi_{k|k'}$ bilden nun zusammen die gesuchte zyklische Minimalbasis lm-ten Grades. Denn wie bereits bemerkt, dulden sie sämtlich S, erzeugen also zunächst einen Teilkörper des zu S gehörigen Invariantenkörpers. Sie erzeugen aber auch diesen gesamten Körper, weil der Körper der Unbestimmten $x_{i|j}$ selbst vom lm-ten Grade über ihnen ist. Denn durch Auflösung je einer zyklischen Gleichung l-ten und m-ten Grades gewinnt man die Größen y_i (2) und $z_{0|j}$ (7) alsdann durch Auflösen der linearen Gleichungssysteme (5) und weiterhin (4) nach den Größen $z_{k|j}$ bezw. $\bar{x}_{i|j}$ die letzteren Größen, schließlich aus (3) die $x_{i|j}$ selbst. Wir haben dabei nur noch zu zeigen, daß die Systeme (4) und (5) stets eindeutige Lösungen besitzen. Nun können wir aber (4) und (5) offenbar folgendermaßen als Matrizengleichungen schreiben:

$$(4') \quad \begin{bmatrix} z_{0|0} & z_{0|1} & \cdots & z_{0|m-1} \\ z_{1|0} & z_{1|1} & \cdots & z_{1|m-1} \\ \cdots & \cdots & \cdots & \cdots \\ z_{l-1|0} & z_{l-1|1} & \cdots & z_{l-1|m-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ y_0 & y_1 & \cdots & y_{l-1} \\ \cdots & \cdots & \cdots & \cdots \\ y_0^{l-1} & y_1^{l-1} & \cdots & y_{l-1}^{l-1} \end{bmatrix} \begin{bmatrix} \bar{x}_{0|0} & \bar{x}_{0|1} & \cdots & \bar{x}_{0|m-1} \\ \bar{x}_{1|0} & \bar{x}_{1|1} & \cdots & \bar{x}_{1|m-1} \\ \cdots & \cdots & \cdots & \cdots \\ \bar{x}_{l-1|0} & \bar{x}_{l-1|1} & \cdots & \bar{x}_{l-1|m-1} \end{bmatrix},$$

$$(5') \quad \begin{bmatrix} \varphi_{1|0} & \varphi_{1|1} & \cdots & \varphi_{1|m-1} \\ \varphi_{2|0} & \varphi_{2|1} & \cdots & \varphi_{2|m-1} \\ \cdots & \cdots & \cdots & \cdots \\ \varphi_{l-1|0} & \varphi_{l-1|1} & \cdots & \varphi_{l-1|m-1} \end{bmatrix} = \begin{bmatrix} z_{1|0} & z_{1|1} & \cdots & z_{1|m-1} \\ z_{2|0} & z_{2|1} & \cdots & z_{2|m-1} \\ \cdots & \cdots & \cdots & \cdots \\ z_{l-1|0} & z_{l-1|1} & \cdots & z_{l-1|m-1} \end{bmatrix} \begin{bmatrix} z_{0|0} & z_{0|1} & \cdots & z_{0|m-2} & z_{0|m-1} \\ z_{0|1} & z_{0|2} & \cdots & z_{0|m-1} & z_{0|0} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ z_{0|m-1} & z_{0|0} & \cdots & z_{0|m-3} & z_{0|m-2} \end{bmatrix} .$$

Die Determinante der Transformationsmatrix in (4′) ist also das Differenzenprodukt der y_i und somit bei „*unbestimmten*“ $x_{i|j}$ von Null verschieden, die in (5′) dagegen, d. h. natürlich die Determinante des *zweiten* Faktors der rechten Seite, verschwindet immer, denn als sogenannte „zyklische“ Determinante hat sie bekanntlich den Wert

$$(9)\quad D = (-1)^{\frac{(m-1)(m-2)}{2}} \prod_{j=0}^{m-1} (z_{0|0} + \varepsilon^j z_{0|1} + \varepsilon^{2j} z_{0|2} + \cdots + \varepsilon^{(m-1)j} z_{0|m-1}),$$

wo ε eine primitive m-te Einheitswurzel bedeutet. Von den Faktoren der rechten Seite verschwindet aber nach (6′) der erste, den man für $j = 0$ erhält. Trotzdem läßt aber (5) stets eine eindeutige Auflösung nach den $z_{k|j}$ zu. Man zeigt dies wohl am einfachsten, indem man in der soeben betrachteten Transformationsmatrix von (5′) jedes Element um 1 vermehrt. Hierdurch wird die rechte Seite von (5′) wegen (6) nicht geändert, die Determinante der Transformationsmatrix aber wird

$$(10)\quad D' = (-1)^{\frac{(m-1)(m-2)}{2}} m \prod_{j=1}^{m-1} (z_{0|0} + \varepsilon^j z_{0|1} + \varepsilon^{2j} z_{0|2} + \cdots + \varepsilon^{(m-1)j} z_{0|m-1}),$$

wie man sofort erkennt, wenn man in (9) die $z_{0|j}$ durch $z_{0|j} + 1$ ersetzt und beachtet, daß $1 + \varepsilon^j + \varepsilon^{2j} + \cdots + \varepsilon^{(m-1)j}$ gleich m wird für $j = 0$, jedoch verschwindet für $1 \leqq j \leqq m - 1$. Nach (7′) wird aber für $\varepsilon^j \neq 1$

$$z_{0|0} + \varepsilon^j z_{0|1} + \cdots + \varepsilon^{(m-1)j} z_{0|m-1} = \sum_i x_{i|0} + \varepsilon^j \sum_i x_{i|1} + \cdots + \varepsilon^{(m-1)j} \sum_i x_{i|m-1}\ ,$$

so daß also die Faktoren von (10) bei „*unbestimmten*“ $x_{i|j}$ nicht verschwinden, d. h. $D' \neq 0$, w. z. b. w.

4. Die zyklischen Minimalbasen sind, abgesehen von dem trivialen Falle $n = 2$, bisher bekannt für $n = 4$ (implizite schon bei Abel angegeben), für die Primzahlgrade 3, 5, 7, 11 [3]) sowie 13, 17, 19, 23 [4]), und gemäß Fußnote 2 für die doppelten Grade, jedoch noch nicht für $n = 8$. Es können daher nach dem obigen Verfahren für eine ganze Reihe zusammengesetzter Grade nunmehr die zyklischen Minimalbasen angegeben werden. Von besonderer Bedeutung ist, daß dies auch für $n = 12$ gilt, weil damit nach B. Seite 41 auch *die sämtlichen metazyklischen Minimalbasen* 13. *Grades angegeben* und also auch die Koeffizienten der auflösbaren Gleichungen 13. Grades, nach deren Galoisschen Gruppen getrennt, durch 13 unabhängige Parameter dargestellt werden können.

[3]) Vgl. B. und F., für $n = 3$ und $n = 4$ auch die dort angegebene Literatur.

[4]) Vgl. B. — Es sei gestattet, bei dieser Gelegenheit kurz auf das Verhältnis der Arbeit von Herrn Furtwängler — die Arbeit ist *nach* meinem Innsbrucker Vortrag über das gleiche Thema, aber *vor* B. erschienen; die Untersuchungen darüber lagen aber, wie in der Einleitung zu F. bemerkt wird, schon länger zurück; Verfasser wurde erst vor kurzem durch Fräulein Noether in liebenswürdiger Weise auf die in F. enthaltenen Untersuchungen zu den metazyklischen Minimalbasen aufmerksam gemacht — zu verschiedenen Arbeiten des Verfassers einzugehen. Hauptgegenstand von F. ist ebenso wie bei B. die Bestimmung der metazyklischen Minimalbasen von Primzahlgrad, auch wird in F. die in B. § 3 als „spezielle S-Basis zweiter Art“ bezeichnete Minimalbasis auf *prinzipiell* die gleiche Art bestimmt. Es fehlt jedoch die in B. § 1 angegebene allgemeine Reduktion des Basisproblems auf $\frac{p-1}{2}$ Unbestimmte, damit auch die in B. § 2 angegebene „spezielle S-Basis erster Art“, und das in B. angegebene Verfahren trägt deshalb — weil für die Existenz einer Basis zweiter Art zusätzliche zahlentheoretische Bedingungen zu denen für die Basis erster Art treten — weiter als das in F. angegebene; vgl. die im Text aufgeführten Zahlenbeispiele. — Das Verfahren in F. zur Zurückführung der zyklischen Minimalbasis $2(2k+1)$-ten Grades auf die vom Grade $2k+1$ nimmt zwar Bezug auf das entsprechende Verfahren des Verfassers, verdient aber den Vorzug vor diesem, weil es sich zu dem hier angegebenen Verfahren verallgemeinern läßt. — Dagegen ist der in F. eingeschlagene Weg zur Bestimmung der Minimalbasis für eine intransitive, auf mehrere Reihen von Unbestimmten bezügliche Permutationsgruppe $\mathfrak{G}_{xyz}\ldots$, welche holoedrisch isomorph zu einer $\mathfrak{G}_x$ ist, nur unwesentlich verschieden von dem Verfahren, das Verfasser kurz vorher in „Beiträge zur Algebra 2: Zur Theorie der metazyklischen Gleichungen von Primzahlgrad“, Sitzungsber. d. Heidelberger Akad. d. Wiss., Math.-Naturw. Kl., 1925, 5. Abhdlg. angegeben hatte.

Schon bei Herleitung der zyklischen Minimalbasis 12. Grades treten alle Besonderheiten des hier angegebenen Verfahrens deutlich hervor. Auf die Durchrechnung dieses Zahlenbeispiels möge trotzdem hier verzichtet werden. Setzt man dagegen, in Behandlung des schon früher erledigten Falles, $l \equiv 1 \pmod 2$, $m = 2$, so erhält man die in F. angegebene Basis. Die Formeln werden hier zwar, wie man leicht sieht, zu sehr spezialisiert, um noch als Beispiel für das Verfahren dienen zu können, immerhin haben sie den Ausgangspunkt für obige Untersuchungen gebildet.

Karlsruhe, September 1930.

Eingegangen 8. Oktober 1930.

Zusatz während der Drucklegung.

Es möge hier auch noch eine *zyklische Minimalbasis* 9. *Grades* angegeben werden, wenn auch ihre Gewinnung ein ganz anderes Problem stellt als das im vorstehenden behandelte. Eine ausführliche Darstellung der Herleitung sowie die Verallgemeinerung des Verfahrens sollen einer besonderen Arbeit vorbehalten bleiben. Hier sei nur bemerkt, daß der Weg durchaus dem parallel verläuft, den der Verfasser in B. zur Bestimmung der zyklischen Minimalbasen von Primzahlgrad angegeben hat, daß insbesondere auch hier „Minimalbasen erster und zweiter Art" unterschieden werden können. Wir geben im folgenden eine „Minimalbasis zweiter Art" an.

Sei ε eine primitive 9. Einheitswurzel,

$$k_\mu = (\varepsilon^{2^\mu}, x) = x_0 + \varepsilon^{2^\mu} x_1 + \varepsilon^{2\cdot 2^\mu} x_2 + \cdots + \varepsilon^{8\cdot 2^\mu} x_8 \qquad (\mu = 0, 1, \ldots, 5),$$

$$h_\varkappa = (\varepsilon^{3^\varkappa}, x) = (x_0 + x_3 + x_6) + \varepsilon^{3^\varkappa}(x_1 + x_4 + x_7) + \varepsilon^{6^\varkappa}(x_2 + x_5 + x_8) \qquad (\varkappa = 0, 1, 2),$$

so multipliziert sich k_μ, wenn man die Unbestimmten x_ν in der Reihenfolge

$$S = (x_0, x_1, \ldots, x_8) \tag{15}$$

vertauscht, mit ε^{-2^μ}, desgleichen $h_\varkappa$ mit $\varepsilon^{-3^\varkappa}$. Daher dulden die neun Funktionen

$$\begin{aligned} v_\mu &= k_\mu\, k_{\mu+3}^{-1}\, k_{\mu+4}\ ^{5}) && (\mu = 0, 1, \ldots, 5)\\ w_1 &= k_1\, k_3\, k_5\, h_1\\ w_2 &= k_0\, k_2\, k_4\, h_2\\ &\text{und } h_0 \end{aligned} \tag{16}$$

die Vertauschung S. Der von ihnen erzeugte Körper umfaßt aber auch die zyklischen Funktionen der x_ν überhaupt, weil er vom 9. Grade über dem Körper dieser Unbestimmten selbst ist. Das Letztere folgt aus den Beziehungen

$$k_0^9 = v_0^2\, v_1\, v_2^5\, v_3^{-2}\, v_4^{-1}\, v_5^4,$$

$$k_0^2\, k_1^{-1} = v_2\, v_3^{-1}\, v_5,$$

denn mit Hilfe der ersten gewinnt man k_0 durch Ausziehen einer 9. Wurzel, aus der zweiten Gleichung und den weiteren, durch zyklische Vertauschung der k_μ und v_μ aus ihr hervorgehenden Gleichungen aber erhält man die übrigen Größen k_μ auf rationalem Wege, endlich dann die h_1, h_2 aus den w_1, w_2 nach (16) gleichfalls auf rationalem Wege.

Von den Größen (16) besitzt nun allein $h_0 = \Sigma x_\nu$ rationale Koeffizienten. Setzt man aber

---

[5]) Die Indizes der k sind stets auf den kleinsten nicht negativen Rest mod. 6 zu reduzieren.

$$(17)\qquad \begin{bmatrix} V_0 \\ V_1 \\ \cdot \\ V_5 \end{bmatrix} = \begin{bmatrix} \varepsilon + \varepsilon^3, & \varepsilon^2 + \varepsilon^6, & \varepsilon^4 + \varepsilon^3, & \varepsilon^8 + \varepsilon^6, & \varepsilon^7 + \varepsilon^3, & \varepsilon^5 + \varepsilon^6 \\ \varepsilon^5 + \varepsilon^6, & \varepsilon + \varepsilon^3, & \varepsilon^2 + \varepsilon^6, & \varepsilon^4 + \varepsilon^3, & \varepsilon^8 + \varepsilon^6, & \varepsilon^7 + \varepsilon^3 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \varepsilon^2 + \varepsilon^6, & \varepsilon^4 + \varepsilon^3, & \varepsilon^8 + \varepsilon^6, & \varepsilon^7 + \varepsilon^3, & \varepsilon^5 + \varepsilon^6, & \varepsilon + \varepsilon^3 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \cdot \\ v_5 \end{bmatrix},$$

ferner

$$(18)\qquad W_1 = \varepsilon^3 w_1 + \varepsilon^6 w_2, \quad W_2 = \varepsilon^6 w_1 + \varepsilon^3 w_2,$$

so ändern sich die Größen V_μ, W_1, W_2 nicht, wenn man ε durch ε^2 ersetzt, sie haben also rationale Koeffizienten. Da schließlich die Gleichungen (17), (18) eindeutig nach den v_μ, w_1, w_2 aufgelöst werden können, weil — wie man leicht erkennt — die zyklischen Determinanten dieser Systeme nicht verschwinden, so bilden die Größen V_μ, W_1, W_2, h_0 eine rationale zyklische Minimalbasis 9. Grades, w. z. b. w.

Es ergibt sich hieraus, daß auch für die metazyklische Gruppe 19. Grades und ihre sämtlichen Untergruppen rationale Minimalbasen angegeben werden können, ganz ebenso, wie wir dies im vierten Abschnitt der vorstehenden Arbeit für die Gruppen 13. Grades erwähnt haben.

Wir bemerken endlich noch, daß die Indizes der Größen k_μ bei der Vertauschung

$$(19)\qquad T = \begin{pmatrix} x_\nu \\ x_{5\nu} \end{pmatrix}$$

in der Reihenfolge

$$(20)\qquad U = (0,\ 1,\ 2,\ 3,\ 4,\ 5),$$

die Größen h_1, h_2 jedoch miteinander vertauscht werden. Entsprechendes gilt infolgedessen für die Größen v_μ bzw. w_1, w_2 und schließlich auch für die V_μ bzw. W_1, W_2. Die Größen

$$(21)\qquad \begin{aligned} \varphi_6 &= V_0 V_2 V_4 \cdot W_1 + V_1 V_3 V_5 \cdot W_2 \\ \varphi_7 &= V_1 V_3 V_5 \cdot W_1 + V_0 V_2 V_4 \cdot W_2 \end{aligned}$$

sowie h_0 dulden daher T. Bilden nun noch die sechs Funktionen

$$(22)\qquad \varphi_\mu(V_0, V_1, \ldots, V_5) \qquad (\mu = 0, 1, \ldots, 5)$$

eine Minimalbasis für den Invariantenkörper der durch U oder U^2 oder U^3 erzeugten Permutationsgruppe der V_μ, so bilden sie, wie man leicht erkennt, zusammen mit den Größen φ_6, φ_7, h_0 auch eine Minimalbasis für die durch S (15) und T (19), bzw. S und T^2 bzw. S und T^3 erzeugte Gruppe. Da die Funktionen (22) aber schon lange bekannt sind, so kann man also auch für die volle lineare Permutationsgruppe 9. Grades und alle ihre Untergruppen, ganz wie bei Gruppen von Primzahlgrad, rationale Minimalbasen angeben.

Karlsruhe, 25. Januar 1931.

Eingegangen 3. Februar 1931.

Bemerkungen zu einem Satz von Stickelberger.

Von *Elemér v. Török* in Pécs (Ungarn).

P. Muth zitiert in seinem Werke „Theorie und Anwendung der Elementartheiler“ [1]) folgenden Satz von Stickelberger:

Sind A und B zwei bilineare Formen von je $2n$ Variabelen $x_1, \ldots, x_n, y_1, \ldots, y_n$, ist die Determinante $|\lambda A - B|$ [2]) nicht identisch Null und $\lambda = c$ eine Wurzel der Gleichung $|\lambda A - B| = 0$, sind ferner

$$(\lambda - c)^{e_1}, \quad (\lambda - c)^{e_2}, \ldots$$

die sämtlichen zur Basis $\lambda - c$ gehörenden Elementarteiler [3]) von $|\lambda A - B|$ nach abnehmender Größe der Exponenten geordnet, und entwickelt man $(\lambda A - B)^{-1}$ [4]) nach steigenden Potenzen von $\lambda - c$, so beginnt die Entwickelung mit einem Gliede von der Gestalt

$$H \cdot (\lambda - c)^{-e_1}, \tag{1}$$

wo H eine bilineare Form bedeutet; ist der Rang von $|H|$ gleich r, so ist

$$e_1 = e_2 = \cdots = e_r > e_{r+1}$$ [5]).

Dem Satze folgt ein Beweis von Frobenius, welchen Muth als „Briefliche Mitteilung vom 21. Juni 1898“ zitiert [6]).

Frobenius beweist den Satz zuerst für einen speziellen Fall, darauf für einen allgemeineren und erst dann für den allgemeinen Fall.

Im folgenden wollen wir einen Beweis geben, welcher sowohl betreffs Kürze als auch Durchsichtigkeit der Beweisführung dem Beweise von Frobenius den Vorzug zu verdienen scheint. Der Umweg wird allerdings unter Gebrauch eines Satzes von Frobenius über reguläre Unterdeterminanten [7]) erspart.

Der Gang unseres Beweises ist folgender: Die Reihenentwicklung von $(\lambda A - B)^{-1}$ wird in ihrer durch die Jacobische Transformation [8]) gewonnenen Form durchgeführt, alsdann wird H einer Transformation unterworfen, wobei der Rang ihres Systems sich nicht ändert. Nach dieser Transformation wird unser Satz evident.

---

[1]) P. Muth, Theorie und Anwendung der Elementartheiler, Leipzig 1899.

[2]) d. h. die Determinante der Form $\lambda A - B$.

[3]) l. c. S. 5.

[4]) d. h. die reziproke Form von $\lambda A - B$, vgl. l. c. S. 27.

[5]) l. c. S. 135. Der Satz hat in der Theorie der kongruenten bilinearen Formen eine Anwendung gefunden.

[6]) Nach meinem Wissen ist dies der einzige Beweis des Satzes, welcher in der Literatur vorkommt.

[7]) l. c. S. 7, Satz 1.

[8]) l. c. S. 69—72.

Nun an den Beweis.

1. Im folgenden bezeichnen wir die Adjunkte des Elementes der i-ten Zeile und k-ten Kolonne im Systeme $||\lambda A - B||$ [9]) mit S_{ik}, weiter diejenige Determinante, deren System aus $||{}_i^i\lambda A - B_i^i||$ durch Weglassen der σ ersten Zeilen und Kolonnen hervorgeht mit $S^{(\sigma)}$ [10]); endlich wird die Determinante, deren System aus dem von $S^{(\sigma)}$ dadurch hervorgeht, daß man die $(i-\sigma)$-te Zeile und $(k-\sigma)$-te Kolonne wegläßt, mit $(-1)^{i+k} \cdot S_{ik}^{(\sigma)}$ bezeichnet. Ferner ist $S^{(n)} = 1$ zu setzen.

Nach der Voraussetzung ist S nicht identisch Null, also besitzt sie nach einem Satze von Frobenius [11]) mindestens eine in bezug auf $\lambda - c$ reguläre [11]) Unterdeterminante $(n-1)$-ter Ordnung. Letztere besitzt wieder eine reguläre Unterdeterminante $(n-2)$-ter Ordnung usw. Durch bloße Umbezeichnung der $2n$ Variabelen kann man also erreichen, daß alle Determinanten $S^{(\sigma)}$ in bezug auf $\lambda - c$ regulär werden.

Wird nun die reziproke Form von $\lambda A - B$,

$$(\lambda A - B)^{-1} = \sum \frac{S_{ik}}{S} \cdot x_k y_i \qquad (i, k = 1, 2, \ldots, n),$$

den linearen Substitutionen

$$\left.\begin{aligned} X^{(\sigma)} &= S_{\sigma\sigma}^{(\sigma-1)} \cdot x_\sigma + \cdots + S_{\sigma n}^{(\sigma-1)} \cdot x_n \\ Y^{(\sigma)} &= S_{\sigma\sigma}^{(\sigma-1)} \cdot y_\sigma + \cdots + S_{n\sigma}^{(\sigma-1)} \cdot y_n \end{aligned}\right\} (\sigma = 1, 2, \ldots, n)$$

— der sogenannten Jacobischen Transformation — unterworfen, so wird

$$(\lambda A - B)^{-1} = \sum_{\sigma=1}^{n} \frac{X^{(\sigma)} Y^{(\sigma)}}{S^{(\sigma-1)} S^{(\sigma)}} \cdot \text{ [12])}$$

2. In dieser Form wollen wir jetzt $(\lambda A - B)^{-1}$ nach steigenden Potenzen von $\lambda - c$ entwickeln.

Nach der Voraussetzung sind die zur Basis $\lambda - c$ gehörenden Elementarteiler von S

$$(\lambda - c)^{e_1}, \qquad (\lambda - c)^{e_2}, \ldots,$$

wobei

$$e_1 \geqq e_2 \geqq \cdots.$$

Ist $\lambda - c$ in den Unterdeterminanten $(n-\sigma)$-ter Ordnung mindestens (im regulären $S^{(\sigma)}$ genau) zur l_σ-ten Potenz enthalten, dann ist

$$e_\sigma = l_{\sigma-1} - l_\sigma \qquad (\sigma = 1, 2, \ldots, n;\ l_n = 0) \text{ [13])}. \tag{2}$$

Andererseits ist $S^{(\sigma)}$, ferner $X^{(\sigma)}$ und $Y^{(\sigma)}$ (bei unbestimmten Werten der Variablen x_i, y_i) genau durch die l_σ-te, $S^{(\sigma-1)}$ genau durch die $l_{\sigma-1}$-te Potenz von $\lambda - c$ teilbar [14]). Multipliziert man also den Bruch

$$\frac{X^{(\sigma)} Y^{(\sigma)}}{S^{(\sigma-1)} S^{(\sigma)}}$$

mit $(\lambda - c)^{l_\sigma + l_{\sigma-1} - 2l_\sigma}$, d. h. wegen (2) mit $(\lambda - c)^{e_\sigma}$, dann haben wir ihn vom Faktor $\lambda - c$ ganz befreit. Also ist die Reihenentwickelung des Bruches

---

[9]) d. h. im Systeme der Form $\lambda A - B$.

[10]) Also ist $S^{(0)} = S = |\lambda A - B|$.

[11]) Vergl. Fußnote [7]).

[12]) Vergl. Fußnote [8]).

[13]) l. c. S. 5.

[14]) $S_{\sigma\sigma}^{(\sigma-1)} = S^{(\sigma)}$, also regulär.

$$\frac{X^{(\sigma)}\,Y^{(\sigma)}}{S^{(\sigma-1)}\,S^{(\sigma)}} = \frac{Z_{\sigma 0}}{(\lambda-c)^{e_\sigma}} + \frac{Z_{\sigma 1}}{(\lambda-c)^{e_\sigma-1}} + \cdots \qquad (\sigma = 1, 2, \ldots, n),$$

wobei

$$Z_{\sigma 0} = \left[\frac{X^{(\sigma)}\,Y^{(\sigma)}}{S^{(\sigma-1)}\,S^{(\sigma)}}\;(\lambda-c)^{e_\sigma}\right]_{\lambda=c}$$

bedeutet.

Ist nun

$$e_1 = e_2 = \cdots = e_\varrho > e_{\varrho+1} \geqq e_{\varrho+2} \geqq \cdots \geqq e_n\,, \tag{3}$$

dann ist in (1)

$$H = \sum_{\sigma=1}^{\varrho} Z_{\sigma 0}\,.$$

3. Nun wird die Form H durch die linearen Substitutionen

$$\left.\begin{aligned}
\xi_\sigma &= \left[\frac{X^{(\sigma)}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c} = \left[\frac{S^{(\sigma-1)}_{\sigma\sigma}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c}\cdot x_\sigma + \cdots + \left[\frac{S^{(\sigma-1)}_{\sigma n}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c}\cdot x_n \\
\eta_\sigma &= \left[\frac{Y^{(\sigma)}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c} = \left[\frac{S^{(\sigma-1)}_{\sigma\sigma}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c}\cdot y_\sigma + \cdots + \left[\frac{S^{(\sigma-1)}_{n\sigma}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c}\cdot y_n
\end{aligned}\right\} \quad (\sigma = 1, 2, \ldots, n),$$

– deren Determinanten von Null verschieden sind [15]) – in $\bar{H}$ transformiert. Alsdann erhalten wir

$$\bar{H} = \sum_{\sigma=1}^{\varrho} L_\sigma\,\xi_\sigma\,\eta_\sigma,$$

wobei, mit Rücksicht auf (2),

$$L_\sigma = \left[\frac{(\lambda-c)^{l_\sigma-1}}{S^{(\sigma-1)}}\cdot\frac{(\lambda-c)^{l_\sigma}}{S^{(\sigma)}}\right]_{\lambda=c} \neq 0 \qquad (\sigma = 1, 2, \ldots, \varrho)$$

ist.

Der Rang des Systems der Form $\bar{H}$ ist infolgedessen gleich ϱ. Da aber die Systeme von H und $\bar{H}$ im Range übereinstimmen, folgt unserer Bezeichnung gemäß

$$\varrho = r,$$

also wegen (3)

$$e_1 = e_2 = \cdots = e_r > e_{r+1}\,,$$

w. z. b. w.

---

[15]) Die Determinante beider Substitutionen ist

$$\prod_{\sigma=1}^{n}\left[\frac{S^{(\sigma-1)}_{\sigma\sigma}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c} = \prod_{\sigma=1}^{n}\left[\frac{S^{(\sigma)}}{(\lambda-c)^{l_\sigma}}\right]_{\lambda=c} \neq 0\,.$$

Eingegangen 16. Oktober 1930.

Verallgemeinerung der in meiner Arbeit: „Ein Satz über trigonometrische Polynome mit Lücken und seine Anwendung in der Theorie der Fourier-Reihen", Journal für die reine und angewandte Math. Bd. 163 bewiesenen Sätze.

Von *S. Sidon* in Budapest.

Durch selbstverständliche Modifikationen des Beweises des Satzes I der im Titel genannten Arbeit ergibt sich folgende Verallgemeinerung desselben:

Ist $\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots$ *eine unendliche reelle Zahlenfolge von der Beschaffenheit, daß in der Folge* $u_{11} = 2\lambda_1$, $u_{12} = \lambda_1 + \lambda_2$, $u'_{12} = \lambda_1 - \lambda_2, \ldots, u_{mn} = \lambda_m + \lambda_n$, $u'_{mn} = \lambda_m - \lambda_n, \ldots$ *die Anzahl der gleichen Glieder unter einer von* m, n *unabhängigen, festen, endlichen Schranke bleibt, so gilt für das verallgemeinerte trigonometrische Polynom*

$$P_n(x) = \sum_{k=1}^{n} (a_k \cos \lambda_k x + b_k \sin \lambda_k x)$$

die Ungleichung

$$[\sum_{k=1}^{n} (a_k^2 + b_k^2)]^{\frac{1}{2}} < C \lim_{T=\infty} \frac{1}{T} \int_{-T}^{T} |P_n(x)|\, dx \,^{1}) .$$

Ein Korollar dieses Satzes ist:

Es sei für die Folge der reellen Zahlen $\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots$ *eine der Bedingungen erfüllt: A. lineare Unabhängigkeit, B. von einem gewissen n an* $\frac{\lambda_{n+1}}{\lambda_n} > q > 1$. *Ist dann* $\sum_{n=1}^{\infty} A_n e^{i\lambda_n x}$ *die Fourier-Reihe einer nach Lebesgue integrierbaren im Stepanoffschen Sinne* [2]) *quasi-periodischen Funktion* $f(x)$, *so ist* $\sum_{n=1}^{\infty} |A_n|^2$ *konvergent.*

Beweis: Die Bedingungen A. und B. sind offenbar Spezialfälle der Bedingung, die die Exponenten in dem für verallgemeinerte trigonometrische Polynome oben ausgesprochenen Satze zu erfüllen haben. Es gilt also, wenn $\sum_{k=1}^{n} A_k e^{i\lambda_k x} = s_n(x)$ gesetzt wird, für jedes n

$$\sum_{k=1}^{n} |A_k|^2 < C \lim_{T=\infty} \frac{1}{T} \int_{-T}^{T} |s_n(x)|\, dx .$$

Nun ist im Falle A. [3])

---

[1]) C bedeutet auch in dieser Arbeit immer eine von n unabhängige, positive Konstante.

[2]) Stepanoff, Über einige Verallgemeinerungen der fastperiodischen Funktionen. Math. Annalen **95** (1926), S. 473—498.

[3]) Bochner, Fastperiodische Funktionen. Math. Annalen **96** (1926), S. 119—147.

$$s_n(x) = \lim_{T=\infty} \frac{1}{T} \int_{-T}^{T} f(t) \prod_{k=0}^{[n]} [1 + \cos \lambda_k (x - t)]\, dt\,,$$

im Falle B. [3])

$$s_n(x) = \lim_{T=\infty} \frac{1}{T} \int_{-T}^{T} f(t) \sum_{r=0}^{i-1} \prod_{k=0}^{\left[\frac{n}{i}\right]} [1 + \cos \lambda_{ik+r} (x - t)]\, dt\,,$$

wo i den Ungleichungen genügt

$$q^i > 3, \quad 1 + \frac{1}{q^i - 1} < q.$$

Daher gilt in beiden Fällen

$$\lim_{T=\infty} \frac{1}{T} \int_{-T}^{T} |s_n(x)|\, dx < C \lim_{T=\infty} \frac{1}{T} \int_{-T}^{T} |f(x)|\, dx\,.$$

$\sum_{k=1}^{n} |A_k|^2$ bleibt also unter einer von n unabhängigen Schranke, womit unsere Behauptung bewiesen ist.

[4]) Sidon, Verallgemeinerung eines Satzes über die absolute Konvergenz von Fourier-Reihen mit Lücken. Math. Annalen **97** (1927), S. 675—676.

Eingegangen 24. November 1930.

Berichtigung zu meiner Arbeit [1])
„Über die Darstellungen einer Zahl als Differenz von zwei Produkten".

Von *Theodor Estermann* in London.

Beim Beweise des Hilfssatzes 7 habe ich einen Fehler gemacht, der sich dadurch berichtigen läßt, daß im Hilfssatz 6 und in seinem Beweise und in (72) $\log t$ überall (im ganzen an sechs Stellen) durch $\log(2t)$ ersetzt wird.

[1]) Journal für Mathematik **164** (1931), 137—182.

Eingegangen 25. Juni 1931.

Mitteilung.

Dem von dem Internationalen Mathematikerkongreß in Bologna 1928 gefaßten Beschluß entsprechend wird vom 4. bis 12. September 1932 in Zürich ein

Internationaler Mathematikerkongreß

stattfinden, auf den das Organisationskomitee bereits jetzt hinweist. Die ersten genaueren Mitteilungen und Einladungen werden im Oktober 1931 verschickt.

Das vorgesehene wissenschaftliche Programm besteht aus einer größeren Reihe von allgemeinen Vorträgen, durch die ein möglichst vollständiges Bild des gegenwärtigen Standes der Mathematik gegeben werden soll, und aus Sektionssitzungen, die für kürzere Mitteilungen über Ergebnisse neuer Untersuchungen bestimmt sind.

Neben diesen Fachveranstaltungen sind gesellschaftliche Zusammenkünfte und Ausflüge, für die die Schweiz besonders schöne Gelegenheiten bietet, geplant, die, wie wir hoffen, zur Förderung und Vertiefung der wissenschaftlichen und persönlichen Beziehungen zwischen den hier versammelten Mathematikern aller Länder beitragen werden.

Zürich, Sommer 1931. Das Organisationskomitee.

Eingegangen 20. Juli 1931.

Mitteilung.

Die Göttinger Gesellschaft der Wissenschaften hat neuerdings einen Vertrieb von Sonderabdrucken eingerichtet, der nach Fachgruppen geordnet ist. Die Fachgruppen der mathematisch-naturwissenschaftlichen Klasse sind:

I. Mathematik; II. Physik, Astronomie, Technik; III. Chemie, einschl. Physikalische Chemie; IV. Geologie und Mineralogie; V. Geographie und Geophysik; VI. Biologie.